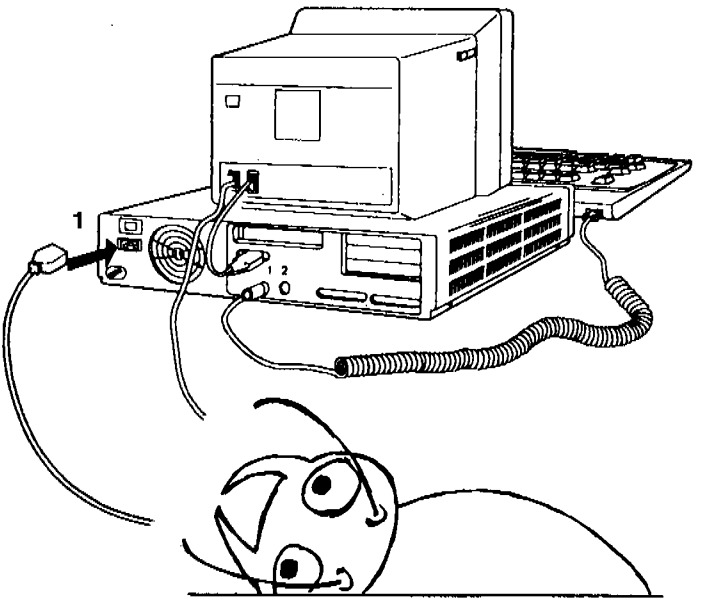


استفاده از میکرو کامپیوترها*
حفظ سیستم های کامپیوتری درمقابل
" ویروس" های نرم افزاری

مجید میراسکندری

اغلب میکرو کامپیوترها در مقابل ویروس‌های نرم افزاری که پرونده های مهم سیستم را خراب میکنند ، آسیب‌پذیرند.
رابرت برواملی (CPA ، PHD) دانشیار رشته سیستم های حسابداری دانشگاه مرکزی میشیگان ، طرز کار این "ویروس" ها و روش‌حفظ سیستم های کامپیوتری از آنها را از آنها شرح میدهد .

چون بسیاری از سیستمهای کامپیوتری قربانی شیطنت " ویروس" های نرم افزاری شده‌اند ، این ویروسها توجه افزاینده‌ای را بخود جلب کرده‌اند . این مزاحمها عملکرد میکرو کامپیوترها را دربعضی موارد بحالت نیمه تعطیل کشانده در بقیه موارد برنامه ها و اطلاعات آنها را از بین برده‌اند .

---

* بنقل از JOURNAL OF ACCOUNTANCY، DEC 1988

" ویروس " نرم افزار معمولا" شامل چند صد واحد " کد زبان ماشین " (۱) است که توسط یک خرابکار و در قالب " برنامه " تنظیم شده ، در شبکه کامپیوتری محلی و یا تابلوی اطلاعات همگانی (bulletin board) جاگذاری میشود . البته در جائی از شبکه که احتمال دارد توسط بسیاری از استفاده کنندگان کپی شود . وقتی برنامه به کامپیوتر منتقل شده مورد استفاده قرارمیگیرد ، " ویروس " به طور موقتی اجرای برنامه اصلی را به تعویق انداخته و از فرصت بدست آمده برای کپی کردن (انتقال) خود به یکی از پرونده های سیستم عامل DOS (۲) مثل COMMAND. COM (که اجرای دستورات DOS را کنترل میکند) ، روی دیسک فعال استفاده مینماید . (۳)

آزمون " ویروس " ها

" ویروس " های شناخته شده حالات مختلفی دارند و خسارتهای خود را به طرق مختلف تحمیل میکنند ، البته در ارائه توضیحات روشنگرانه در خصوص نحوه اشاره و روش انتقامی آنها " اما " و " اگر " های زیادی هست .

---

1 - MACHINE LANGUAGE CODE
2 - DISK OPERATING SYSTEM
۳ - سیستم عامل متکی به دیسک (DOS) خود نرم افزاری است که اجازه میدهد امکانات مختلف کامپیوتر مورد استفاده قرار گیرد . هر کامپیوتر سیستم عامل خود را دارد و هیچ کامپیوتری بدون آن کار نمیکند . امکانات این نرم افزار معمولا" محرمانه است ورود به این نرم افزار و خرابکاری در آن باعث بروز مشکلات اساسی در عملکرد دستورات مهم عملیاتی آن میگردد . م -

وقتی کامپیوتری را که حاوی سیستم عامل آلوده (روی دیسک فعال خود) میباشد . روشن کنیم ، ویروس به حافظه اصلی منتقل میشود . سپس هر گاه از یکی از دستورات معمولی DOS مثل dir (۴) ، copy (۵) ، type (۶) استفاده کنیم ، " ویروس " فعال شده خود را روی پرونده های دیسک دیگر منتقل نموده و منتظر باقی میماند برای مثال فرض کنیم خرابکار مورد نظر ویروس خود را بصورت تاریخ مشخص جا گذاری کرده باشد ، وقتی تاریخ تقویمی کامپیوتر به تاریخ مورد نظر خرابکار برسد ویروس فعال شده پرونده های اساسی سیستم را خراب میکند مثل پرونده فهرست راهنما (directory) یا تابلوی تسهیم پرونده ها (file allocation table) (این فایلها دسترسی و بایگانی کلیه پرونده های موجود روی دیسک را هماهنگ میکنند) . نتیجه حاصله ، دیسکی غیر قابل دسترس یا استفاده خواهد بود . برنامه ها و اطلاعات ضبط شده روی این دیسک را نمیتوان بدون کمک طاقت فرسای تعمیر سیستم ، خواند یا کپی کرد .

خسارت بهمین جا خاتمه نمی یابد . چون "ویروس" خود را روی دیسک ها و حتی کامپیوترهای دیگر منتقل کرده است . تا کنون ویروس ها خود را به سیستم های با کنترل ایمنی خوب هم منتقل کرده اند ، محدود کردن آنها نیز بسیار مشکل شده زیرا اکثر استفاده کنندگان از کامپیوتر درک کامل از dos یا "ویروس" ها ندارند و ابزارهایی که برای حفاظت سیستم های کامپیوتری طراحی شده نیز بسیار جدیدند .

---

۴ - dir مخفف directory و با این دستور سیستم عامل فهرست پرونده ها و برنامه های موجود روی دیسک فعال را نشان داده یا چاپ میکند . م

۵ - copy - دستوری است که سیستم عامل یک پرونده یا یک برنامه را از روی دیسکی به روی دیسک دیگر باز نویسی میکند . م

۶ - type دستوری است که با آن سیستم عامل محتویات یک پرونده را روی صفحه نمایش منتقل میکند . م

موارد جدید شیوع ویروس

این اواخر موارد متعددی از حملات ویروسی مهم گزارش‌شده است . تا کنون شعور متعارف حاکی از این فرضیات بوده است:

۱) سیستمهای کوچک فقط از طریق برنامه‌های ضبط شده از تابلوی اطلاعات همگانی کامپیوتری آلوده شده‌اند .

۲) نرم افزارهای آماده تجارتی که میتوان آنها را از خرده فروشان معمولی تهیه کرد سالم بنظر میرسند.

۳) بنظر میرسد پرونده های قابل اجرا تنها محمل سرایت باشند .

تجربیات واقعی بسیاری از استفاده کنندگان میکرو کامپیوترها نشان میدهد که فرضیات فوق نیز میتواند بنحو خطرناکی گمراه کننده باشد.

یکی از ویروسها عامل موثر درخرابی بسته نرم افزاری (۷) برنامه های گرافیکی پرونده های خرده فروشی یک شرکت و دیگری خرابکار پرونده اطلاعات یکی از شبکه های مخابراتی داخلی شناخته شده است .

خسارتهای ناشی از این همه گیری مختلف بوده است . ویروسی که به پرونده شبکه مخابراتی نفوذ کرده بود باعث نمایش یک موضوع غیر مرتبط میشد ضمن اینکه مرتبا" به تولید مثل از طریق تقسیم سلولی ادامه میداد. ولی بعضی از آنها بسیار شریرند . سیستم کامپیوتری یکی ازدانشکاهها مورد حمله ویروسی قرارگرفت که خود را روی تمام نسخه های یکی از پرونده های سیستم عامل پخش کرده بود . سپس تمام پرونده های سیستم روی دیسک را خراب نموده بود .این عمل باعث خسارتهای جدی به کلیه اطلاعات شد بطوریکه تمام آنها را بی استفاده کرد بطوری که هیچ کاری غیراز " تجدید ساختار" (۸) دیسک اصلی نمیشد کرد .

---

۷ - package

۸ - Reformat - عملی است که با آن دیسک را قطاع بندی و شیاربندی میکنند . تمام دیسکهای موجود برای بار اول بایستی format شوند و با Refgormat کردن آنها کلیه اطلاعات و برنامه ها قبلی پاک میشود که دو مرتبه تمام اطلاعات و برنامه ها را بایستی روی آن ضبط نمود . م -

در مجموع هیچ استفاده کننده‌ای آسیب ناپذیر نیست . ویروسی بنام scores درموسسه‌ی خدمات مشاوره‌ای سیستم Electronic Data Systems نفوذ کرد و برنامه های ارزشمند و محرمانه تجاری را خراب نمود .

اقدامات حفاظتی

تدابیری برای حفاظت میکروکامپیوترها درمقابل "سرایت ویروسی" میتوان اتخاذ کرد ، اما مهم این است که بدانیم هیچ سیستمی را نمیتوان کاملا" محفوظ تلقی کرد چون تمام اقدامات دفاعی بر اساس حمله های گذشته و بر آورد روشهای برنامه ریزی تولید ویروس در آینده طراحی میگردد روشهای پیشگیری که موثر بوده اند ، روشهایی هستند که یاتوسط استفاده کننده‌های مطلع طراحی شدو یا نرم افزارهایی است . که توسط دانشمندان رشته کامپیوتر نوشته شده است .

اولین و بهترین دفاع تهیه نسخه بدل (۹) از پرونده های اطلاعات و برنامه است . تهیه نسخه های بدل از دیسک های سخت (۱۰) بسیار حیاتی است . جدول زیر مشخصات سه نرم افزارمخصوص تهیه نسخه‌های بدل که بسیار عمومی شده اند را نشان میدهد:

Corefast — $149

Core International, Inc.
7171 North Federal Highway
Boca Raton, Florida 33421
(305) 997-6044

Fastback Plus, Version 1.01 — $189

Fifth Generation Systems, Inc.
11200 Industriplex Boulevard
Baton Rouge, Louisiana 70809
(504) 291-7283

PC-FullBack — $69.95

Westlake Data
P.O. Box 1711
Austin, Texas 78767
(512) 328-1041

---

۹ - back up - معمولا" قبل از استفاده و بروز رساندن پرونده ها یک نسخه از روی اصل آنها تهیه میشود که اگر نسخه مورداستفاده بنحوی خراب شود برنامه‌ها و اطلاعات قبلی روی نسخه بدل محفوظ باشد .م -

۱۰- hard disk دیسک از جنس سخت (غیر قابل انعطاف) که معمولا" از پنج میلیون واحد به بالا اطلاعات را میتوان در آن نگه داشت . م -

سایر اقدامات شامل برنامه های نرم افزاری آزمون و نرم افزارهای فرمت نشده است .

نرم افزارهای آزمون

تمام برنامه های قابل خرید از فروشندگان جزء و برنامه های عمومی بایستی مورد آزمایش قرار گیرند . این آزمایش بایستی روی میکرو کامپیوترهای بدون دیسک سخت صورت پذیرد . دیسکت های مورد استفاده در موقع آزمایش نبایستی مورد استفاده سایر سیستمها واقع گردیده و نبایستی روی دیسک های دیگر یا کامپیوترهای دیگر کپی شوند. این عمل از شیوع ویروس به سیستمهای دیگر جلوگیری خواهد کرد . تمام پرونده های قابل اجرا بایستی توسط یک "ویراستار متن " یا دستور type سیستم عامل dos جهت تشخیص ویروس های شناخته شده ای نظیر BRAIN (مغز) و scores (امتیازات) مورد بررسی دقیق قرار گیرند و متن های مشکوک فاش گردند .

نرم افزار مورد بحث بایستی حداقل ۱۵مرتبه در این محیط بسته مورد استفاده قرار گیرد تا بقدر کافی فرصت مناسب در اختیار ویروس در کمین ، برای ظهور قرار گیرد . عاقلانه است اگر تاریخ موثر موجود در حافظه تغییر داده شود بطوریکه از عملکرد ۳۶۵ روز بعد اطمینان حاصل گردد . دستورات قابل تکراری که تاریخ را عوض کرده و یک دستور dos مثل dir یا type را اجرا می کند درتسهیل این آزمایش موثر است .

این نحوه عمل بایستی ویروس در کمین را تحریک کند البته اگر عملیات خرابکاریش براساس تاریخ طرح ریزی شده باشد . در حقیقت اگر ویروسی موجودباشد هنگام انجام این آزمایش ها ، بایستی حمله خود را آغاز کند . وقتی ویروسی پیدا شد تمام دیسک های آلوده را برچسب بزنید و برای مطالعات بعدی جداگانه نگه دارید ((دیسکهای آلوده را میتوانید برای دکتر هاروند هایلند که تحقیقات مفصلی روی برنامه های ویروس و روشهای ضد ویروس انجام میدهد ارسال نمائید. آدرس او این است :

DR. Highland ، Editor، Computers and Secuvity ، Virus Research 562 Croydon Road، Elmont، New York 11003-2814))

نرم افزارهای فرمت نشده (۱۱)

استفاده از این نرم افزارها احتیاطی عاقلانه است . این نرم افزار اطلاعات اساسی سیستم مثل فهرست و جدول تسهیم پرونده دیسک نسخه بدل تهیه میکند . اگر ویروسی محدوده سیستم دیسک را خراب کرده باشد این برنامه از نسخه بدل اطلاعات برای ذخیره کردن اطلاعات روی دیسک استفاده میکند .این برنامه ها در سیستم های نرم افزاری مختلفی آماده فروش می باشند. دو نوع بسیار مقبول عامه آن عبارتند از :

- Pc-tools Deluxe
- Norton's Utilites

که در تمام مغازه ها خرده فروشی وسایل کامپیوتری موجودند.

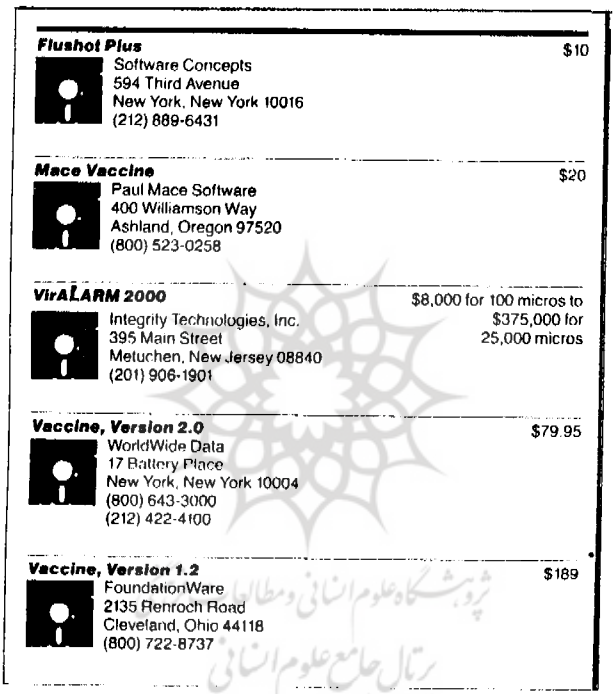
برنامه های ضد " ویروس"

تعداد زیادی برنامه های ضد " ویروس" تاکنون تهیه شده که روی دیسک نصب میشوند .این برنامه ها به وسایل زیرسعی میکنند تاپوشش امنیتی کافی ایجاد نمایند .

- جلوگیری از دسترسی ویروس به دیسک و حافظه جانبی .
- دفع ویروس.
- تعمیر خسارتهای وارده به پرونده های سیستم .

جدول زیر برنامه های ضد ویروس مورد قبول عامه را نشان میدهد . همانطور که دیده میشود قیمتها خیلی باهم اختلاف دارند . هزینه اولی تنها ۱۰ دلار ر قیمت سومی بسته به تعداد میکروکامپیوترهای مورد نظراز ۸۰۰۰ دلار برای ۱۰۰ دستگاه شروع شده به ۳۷۵۰۰۰ دلار را برای ۲۵۰۰۰ دستگاه میرسد.

11- Unformat software



Flushot Plus — $10
Software Concepts
594 Third Avenue
New York, New York 10016
(212) 889-6431

Mace Vaccine — $20
Paul Mace Software
400 Williamson Way
Ashland, Oregon 97520
(800) 523-0258

VirALARM 2000 — $8,000 for 100 micros to $375,000 for 25,000 micros
Integrity Technologies, Inc.
395 Main Street
Metuchen, New Jersey 08840
(201) 906-1901

Vaccine, Version 2.0 — $79.95
WorldWide Data
17 Battery Place
New York, New York 10004
(800) 643-3000
(212) 422-4100

Vaccine, Version 1.2 — $189
FoundationWare
2135 Renroch Road
Cleveland, Ohio 44118
(800) 722-8737

حمایت معقول

نظر به اینکه بسیاری از ویروس‌های معروف ناپایدارند یا خوب شناخته نشده‌اند ، سیستم حمایتی کاملا" مطمئنی وجود ندارد . مضافا" سیستم حمایتی بایستی آنقدر ساده باشد که تمام استفاده کنندگان از میکرو کامپیوتر براحتی از آن استفاده کنند ضمن اینکه از تمام امکانات میکرو کامپیوتر هم برخوردار باشند. بنابراین مطالبی که در این مقاله ذکر گردید را تنها میتوان کوششی در ارائه " سطح معقولی " از " ایجاد حمایت " تلقی نمود .