ckmow.com

License/Legal

Virus Tutorial

Navigation

Misc Terms

Tutorial Map

Anti-Virus Software

Copyright 1996-2002, Computer Knowledge. All Rights Reserved

The Computer Knowledge Virus Tutorial is a copyright product of Computer Knowledge. It also contains copyrighted material from others (used with permission). Please honor the copyrights. Read the tutorial, learn from the tutorial, download and run the PDF version of the tutorial on your computer, link to the tutorial. But, please don't copy it and claim it as your own in whole or part.

The PDF version of the Computer Knowledge Virus Tutorial should be considered freeware. It is **NOT** in the public domain. It is copyrighted by Computer Knowledge and it and all accompanying materials are protected by United States copyright law and also by international treaty provisions.

The tutorial requires no payment of license fees for its individual use as an educational tool. If you are paying to use the tutorial please advise Computer Knowledge (PO Box 5818, Santa Maria, CA 93456 USA). Please provide contact information for those charging the fee.

License for Distribution of the PDF Version

No royalties are required for distribution so long as distribution charges only cover the costs of such distribution (plus a nominal profit if the distribution channel is a profit-

making channel). Under no circumstances is payment of such fees to be represented or understood to constitute legal ownership of this tutorial or any of its associated files.

Any distribution for profit beyond that described just above requires written permission from Computer Knowledge and payment of negotiated royalties.

You may not use, copy, rent, lease, sell, modify, decompile, disassemble, otherwise reverse engineer, or transfer the licensed program except as provided in this agreement. Any such unauthorized use shall result in immediate and automatic termination of this license.

In no case may this product be bundled with hardware or other software without written permission from Computer Knowledge (PO Box 5818, Santa Maria, CA 93456 USA).

All distribution of the Computer Knowledge Virus Tutorial is further restricted with regard to sources which also distribute virus source code and related virus construction/creation materials. The tutorial may not be made available on any site, CD-ROM, or with any package which makes available or contains viruses, virus source code, virus construction programs, or virus creation material.

Permission to distribute the Computer Knowledge Virus Tutorial program is not transferable, assignable, saleable, or franchisable. Each entity wishing to distribute the package must independently satisfy the terms of this limited distribution license.

You agree that the software will not be shipped, transferred or exported into any country or used in any manner prohibited by the United States Export Administration Act or any other export laws, restrictions or regulations.

U.S. Government Information: Use, duplication, or disclosure by the U.S. Government of the computer software

and documentation in this package shall be subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7013 (Oct 1988) and FAR 52.227-19 (Jun 1987). The Contractor is Computer Knowledge, PO Box 5818, Santa Maria, CA 93456-5818 USA.

Warranty

Limited warranty: This software is provided on an "as is" basis. Computer Knowledge disclaims all warranties relating to this software, whether expressed or implied, including but not limited to any implied warranties of merchantability or fitness for a particular purpose. Neither Computer Knowledge nor anyone else who has been involved in the creation, production, or delivery of this software shall be liable for any indirect, consequential, or incidental damages arising out of the use or inability to use such software, even if Computer Knowledge has been advised of the possibility of such damages or claims. The person using the software bears all risk as to the quality and performance of the software.

Some jurisdictions do not allow limitation or exclusion of incidental or consequential damages, so the above limitations or exclusion may not apply to you to the extent that liability is by law incapable of exclusion or restriction.

In no event shall any theory of liability exceed the license fee paid to Computer Knowledge.

This agreement shall be governed by the laws of the State of California excluding the application of its conflicts of law rules and shall inure to the benefit of Computer Knowledge and any successors, administrators, heirs and assigns. Any action or proceeding brought by either party against the other arising out of or related to this agreement shall be brought only in a STATE or FEDERAL COURT of competent jurisdiction located in Santa Barbara County, California. The parties hereby consent to in personam jurisdiction of said

courts.

You agree and acknowledge that you will thoroughly inspect and test the software for all of your purposes upon commencement of your use. Any suit or other legal action, claim or any arbitration relating in any way to this agreement or software covered by it must be officially filed or officially commenced no later than three months (90 days) after your first use of the software.

This agreement will not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded.

General

All rights not expressly granted here are reserved to Computer Knowledge.

Computer Knowledge may revoke any permissions granted here, by notifying you in writing.

If any part of this agreement is found void and unenforceable, it will not affect the validity of the balance of the agreement, which shall remain valid and enforceable according to its terms.

Using this tutorial means that you agree to these terms and conditions. This agreement may only be modified in writing signed by an authorized officer of Computer Knowledge.

Please visit our sponsors.

Click Here to Visit our Sponsor

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2002 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Virus Tutorial

Please visit our sponsors.

Click Here to Visit our Sponsor

Navigation

Tutorial Map

Anti-Virus Software

Computer Knowledge Virus Tutorial

Welcome to the Computer Knowledge tutorial on computer viruses. We'll discuss what they are, give you some history, discuss protection from viruses, and mention some of the characteristics of a virus hoax.

Keep in mind that not everything that goes wrong with a computer is caused by a computer virus or worm. Both hardware and software failure is still a leading cause of computer problems.

If you read each page to the end you should be able to proceed on a page-by-page basis. A "next" button will guide you. To jump to a specific page please visit our map page. A listing of anti-virus software vendors is also available. Links to both of these should appear at the top of each page.

Please also don't forget to read the **License/Legal** info. There are license, use, and distribution requirements for this tutorial, even if it is on the Web.

Virus Introduction… Next

Finally, this tutorial can be downloaded to run on your computer if you have a copy of Adobe Acrobat (a free reader is available). The links below will allow you to download a zip file with the tutorial PDF file in it (if you don't understand the zip compression format please see our info page on this) and/or a copy of the latest Acrobat PDF reader. (*This copy may lag the posted tutorial as it is only updated approximately once a month; or less often if changes were minor.*)

Download Tutorial Zip File (800K)

Download Acrobat Reader

New/updated pages:

- Added a page on virus naming (11 May 2002); new PDF file (18 May 2002)
- Updated recent history; minor corrections; new PDF file (10 Jan 2002)
- Updated recent history; added Nimda description (11 Oct 2001)
- Entire tutorial updated/redesigned (September 2001)

Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small

payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 1996-2002 Computer Knowledge, All Rights Reserved
[Pray the Rosary](#) for peace.

CKNOW.COM

Virus Tutorial

Here you'll find links to any page in the tutorial. The list is organized along the lines of the tutorial so you can see how the information flows.

Navigation

Tutorial Map

Anti-Virus Software

Top Level Pages

- Virus Tutorial Home
- Virus Intro
- Virus Types
- Virus History
- Virus Protection
- Virus Hoaxes
- Current Threats

Introduction to Viruses

- Virus Behaviour
- Number of Viruses
- Virus Names
- How Serious are Viruses?
- Are There Good Viruses?
- Hardware Threats
- Software Threats

Types of Viruses

- [What Viruses Infect](#)
  - [System Sector](#)
  - [File](#)
  - [Macro](#)
  - [Companion](#)
  - [Cluster](#)
  - [Batch File](#)
  - [Source Code](#)
  - [Visual Basic Worms](#)
- [How Viruses Infect](#)
  - [Polymorphic](#)
  - [Stealth](#)
  - [Fast and Slow](#)
  - [Sparse](#)
  - [Armored](#)
  - [Multipartite](#)
  - [Spacefiller](#)
  - [Tunneling](#)
  - [Camouflage](#)
  - [NTFS ADS](#)
- [Virus Droppers](#)

History of Viruses

- [Summary History Page](#)
- [Dr. Solomon's History](#)
  - [1986-1987](#)
  - [1988](#)
  - [1989](#)
  - [1990](#)
  - [1991](#)
  - [1992](#)
  - [1993](#)
  - [The Future](#)

Single Item Pages

- [AV Software](#)
- [License](#)
- [Virus Plural](#)
- [Partition Sector](#)
- [DOS Boot Sector](#)
- [FDISK /MBR](#)
- [False Authority](#)
- [Logic Bombs](#)
- [Trojans](#)
- [Worms](#)

Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

ccknow.com

Anti-Virus Software

Vendors

Virus Tutorial

Please visit our sponsors.

Click Here to Visit our Sponsor

Navigation

Misc.Terms

Tutorial Map

Anti-Virus Software

There are a number of companies that produce anti-virus software. This is not intended to be a complete list of anti-virus companies; but, it is a good starting place.

Anti-Virus Software Companies

(Alphabetical order… position in the list does **not** indicate any recommendation of one over another.)

- **AVG Professional**
- **Command Antivirus**
- **eTrust EZ Armor Suite**
- **F-Secure Anti-Virus**
- **Integrity Master** (a "smart" integrity checker)
- **Kaspersky Anti-Virus**
- **McAfee VirusScan**
- **MIMESweeper** (mail firewall)
- **Norman Virus Control**
- **Norton AntiVirus**
- **Panda Antivirus**
- **Sophos Sweep**
- **Trend PC-cillin**

Free Internet Scanning

If you search on "internet virus scanning" a number of sites pop up. They all seem to link back to the Trend HouseCall service so you might as well go there first…

- http://housecall.antivirus.com/

Disaster Recovery

And, should you catch a virus and it activates with a really nasty payload that effectively erases your hard disk (or, for that matter, you disk fails for any reason) there are companies that will attempt to recover your data if it is important and you have not followed our recommendation to back up frequently. These procedures are labor intensive so you should expect to pay accordingly.

- [Ontrack Data Recovery, Inc.](#)
- [DataRescue](#)

Please visit our sponsors.

[Click Here to Visit our Sponsor](#)

[AV Software](#) | [License](#) | [Virus Plural](#) | [Partition Sector](#) | [DOS Boot Sector](#) | [FDISK /MBR](#) | [False Authority](#) | [Logic Bombs](#) | [Trojans](#) | [Worms](#)
[Virus Tutorial Home](#) | [Virus Intro](#) | [Virus Types](#) | [Virus History](#) | [Virus Protection](#) | [Virus Hoaxes](#) | [Current Threats](#)
[Home](#) | [Products](#) | [Definitions](#) | [Newsletter](#) | [Virus Tutorial](#) | [Contact](#)

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.

[Pray the Rosary](#) for peace.

ckmow.com

Virus Introduction

Virus Tutorial

Navigation

Virus Intro

[Tutorial Map](#)

[Anti-Virus Software](#)

> **A virus reproduces, usually without your permission or knowledge. In general terms they have an infection phase where they reproduce widely and an attack phase where they do whatever damage they are programmed to do (if any). There are a large number of virus types.**

Viruses are a cause of much confusion and a target of considerable misinformation even from some virus "experts." Let's define what we mean by virus:

> **A virus is a program that reproduces its own code by attaching itself to other executable files in such a way that the virus code is executed when the infected executable file is executed.**

You could probably also say that the virus must do this without the permission or knowledge of the user, but that's not a vital distinction for purposes of our discussion here. **We are using a broad definition of "executable file" and "attach" here.**

An obvious example of an executable file would be a program (COM or EXE file) or an overlay or library file used by an EXE file. Less obvious, but just as critical, would be the macro portion of what you might generally consider to be a data file (e.g., a Microsoft Word document). It's important to also realize that the system sectors on either a hard or floppy disk contain executable code that can be infected--even those on a data disk. More recently, scripts written for internet web sites and/or included in E-mail can also be executed and infected.

To attach might mean physically adding to the end of a file, inserting into the middle of a file, or simply placing a pointer to a different location on the disk somewhere where the virus can find it.

Most viruses do their "job" by placing self-replicating code in other programs, so that when those other programs are executed, even more programs are "infected" with the self-replicating code. This self-replicating code, when triggered by some event, may do a potentially harmful act to your computer.

Another way of looking at viruses is to consider them to be programs written to create copies of themselves. These programs attach these copies onto host programs (infecting these programs). When one of these hosts is executed, the virus code (which was attached to the host) executes, and links copies of itself to even more hosts.

Similar to viruses, you can also find malicious code in Trojan Horses, worms, and logic bombs. Often the characteristics of both a virus and a worm can be found in the same beast; confusing the issue even further.

Before looking at specific virus types you might also want to consider the following general discussions:

- **Virus Behavior**. Infect, then attack; common behavior of most viruses.

- [Number of Viruses](#). Lots and lots.
- [Virus Names](#). It's not easy nor standardized.
- [How Serious Are Viruses?](#) Worms spreading due to user inattention are a serious threat.
- [What About Good Viruses?](#) The general consensus is that there are none.
- [Hardware Threats](#). Viruses are not the only things that can cause damage. Consider some hardware problems.
- [Software Threats](#). Viruses are not the only things that can cause damage. Consider some software problems.

Summary

- A virus is a program that reproduces its own code.
- Generally, the first thing a virus does is to reproduce (i.e., infect).
  - Viruses balance infection versus detection possibility.
  - Some viruses use a variety of techniques to hide themselves.
- On some defined trigger, some viruses will then activate.
  - Viruses need time to establish a beachhead, so even if they activate they often will wait before doing so.
  - Not all viruses activate, but all viruses steal system resources and often have bugs that might do destructive things.
- The categories of viruses are many and diverse. There have been many made and if you get one it should be taken seriously. Don't be fooled by claims of a good virus; there is no reason at the moment to create one.

[Virus Behavior](#)…

Please visit our sponsors.

Click Here to Visit our Sponsor

Behaviour | Number | Names | How Serious? | Good Viruses? | Hardware Threats | Software Threats
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

ckhow.com

Virus Types/Methods

Virus Tutorial

Virus Types

> **Viruses come in many types; written using many different infection strategies.**

Viruses come in a variety of types. Breaking them into categories is not easy as many viruses have multiple characteristics and so would fall into multiple categories. We're going to describe two different types of category systems: what they infect and how they infect. Because they are so common, we're also going to include a category specific to worms.

What They Infect

Viruses can infect a number of different portions of the computer's operating and file system. These include:

- System Sectors
- Files
- Macros
- Companion Files
- Disk Clusters
- Batch Files

Navigation

Virus Types

Tutorial Map

Anti-Virus Software

- [Source Code](#)
- [Worms using Visual Basic](#)

How They Infect

Viruses are sometimes also categorized by how they infect. These categorizations often overlap the categories above and may even be included in the description (e.g., polymorphic file virus). These categories include:

- [Polymorphic Viruses](#)
- [Stealth Viruses](#)
- [Fast and Slow Infectors](#)
- [Sparse Infectors](#)
- [Armored Viruses](#)
- [Multipartite Viruses](#)
- [Cavity (Spacefiller) Viruses](#)
- [Tunneling Viruses](#)
- [Camouflage Viruses](#)
- [NTFS ADS Viruses](#)

And, in a special category, one might include:

- [Virus Droppers](#)
  Programs that place viruses onto your system but themselves may not be viruses (a special form of Trojan).

If you know, click on the virus topic you are interested in or read about each in sequence…

[Summary of What Viruses Infect](#)…

What Viruses Infect ||| System Sector | File | Macro | Companion | Cluster | Batch File | Source Code | Visual Basic Worms
How Viruses Infect ||| Polymorphic | Stealth | Fast and Slow | Sparse | Armored | Multipartite | Spacefiller | Tunneling |
Camouflage | NTFS ADS | Virus Droppers
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Virus Tutorial

Navigation

History Detail

Tutorial Map

Anti-Virus Software

Virus History

Narrative histories by Dr. Alan Solomon and Robert M. Slade are available. Below is an expanded summary.

1981 - The First Virus In The Wild

As described in Robert Slade's history, the first virus in the wild actually predated the experimental work that defined current-day viruses. It was spread on Apple II floppy disks (which contained the operating system) and reputed to have spread from Texas A&M. [*Side note*: Thanks to a pointer from anti-virus pioneer Fridrik Skulason we know the virus was named Elk Cloner and displayed a little rhyme on the screen:

```
It will get on all your disks
    It will infiltrate your chips
        Yes it's Cloner!

It will stick to you like glue
    It will modify ram too
        Send in the Cloner!
```

For more info on Elk Cloner see http://www.skrenta.com/cloner/

1983 - The First Documented Experimental Virus

Fred Cohen's seminal paper *Computer Viruses - Theory and Experiments* from 1984 defines a computer virus and describes the experiments he and others performed to prove that the concept of a computer virus was viable. From the paper…

> On November 3, 1983, the first virus was conceived of as an experiment to be presented at a weekly seminar on computer security. The concept was first introduced in this seminar by the author, and the name 'virus' was thought of by Len Adleman. After 8 hours of expert work on a heavily loaded VAX 11/750 system running Unix, the first virus was completed and ready for demonstration. Within a week, permission was obtained to perform experiments, and 5 experiments were performed. On November 10, the virus was demonstrated to the security seminar.

1986 - Brain, PC-Write Trojan, & Virdem

The common story is that two brothers from Pakistan analyzed the boot sector of a floppy disk and developed a method of infecting it with a virus dubbed "Brain" (the origin is generally accepted but not absolutely). Because it spread widely on the popular MS-DOS PC system this is typically called the first computer virus; even though it was predated by Cohen's experiments and the Apple II virus. That same year the first PC-based Trojan was released in the form of the popular shareware program *PC-Write*. Some reports say Virdem was also found this year; it is often called the first file virus.

1987 - File Infectors, Lehigh, & Christmas Worm

The first file viruses started to appear. Most concentrated

on COM files; COMMAND.COM in particular. The first of these to infect COMMAND.COM is typically reported to be the Lehigh virus. At this time other work was done to create the first EXE infector: Suriv-02 (Suriv = Virus backward). (This virus evolved into the Jerusalem virus.) A fast-spreading (500,000 replications per hour) worm hit IBM mainframes during this year: the IBM Christmas Worm.

1988 - MacMag, Scores, & Internet Worm

MacMag, a Hypercard stack virus on the Macintosh is generally considered the first Macintosh virus and the Scores virus was the source of the first major Macintosh outbreak. The Internet Worm (Robert Morris' creation) causes the first Internet crisis and shut down many computers. CERT is created to respond to such attacks.

1989 - AIDS Trojan

This Trojan is famous for holding data hostage. The Trojan was sent out under the guise of an AIDS information program. When run it encrypted the user's hard drive and demanded payment for the decryption key.

1990 - VX BBS & Little Black Book (AT&T Attack)

The first virus exchange (VX) BBS went online in Bulgaria. Here virus authors could trade code and exchange ideas. Also, in 1990, Mark Ludwig's book on virus writing (*The Little Black Book of Computer Viruses*) was published. While there is no proof, hackers are suspected of taking down the AT&T long-distance switching system.

1991 - Tequila

Tequila was the first polymorphic virus; it came out of Switzerland and changed itself in an attempt to avoid detection.

1992 - Michelangelo, DAME, & VCL

Michelangelo was the first media darling. A wordwide alert went out with claims of massive damage predicted. Actually, little happened. The same year the Dark Avenger Mutation Engine (DAME) became the first toolkit that could be used to turn any virus into a [polymorphic](#) virus. Also that year the Virus Creation Laboratory (VCL) became the first actual virus creation kit. It had pull-down menus and selectable payloads.

1995 - Year of the Hacker

Hackers attacked Griffith Air Force Base, the Korean Atomic Research Institute, NASA, Goddard Space Flight Center, and the Jet Propulsion Laboratory. GE, IBM, Pipeline and other companies were all hit by the "Internet Liberation Front" on Thanksgiving.

1995 - Concept

The first [macro virus](#) to attack Word, Concept, is developed.

1996 - Boza, Laroux, & Staog

Boza is the first virus designed specifically for [Windows 95 files](#). Laroux is the first Excel macro virus. And, Staog is the first Linux virus (written by the same group that wrote Boza).

1998 - Strange Brew & Back Orifice

Strange Brew is the first Java virus. [Back Orifice](#) is the first Trojan designed to be a remote administration tool that allows others to take over a remote computer via the Internet. Access macro viruses start to appear.

1999 - Melissa, Corner, Tristate, & Bubbleboy

Melissa is the first combination Word macro virus and worm to use the Outlook and Outlook Express address book to send itself to others via E-mail. It arrived in March. Corner is the first virus to infect MS Project files. Tristate is the first multi-program macro virus; it infects Word, Excel, and PowerPoint files. Bubbleboy is the first worm that would activate when a user simply opened and E-mail message in Microsoft Outlook (or previewed the message in Outlook Express). No attachment necessary. Bubbleboy was the proof of concept; Kak spread widely using this technique.

2000 - DDoS, Love Letter, Timofonica, Liberty (Palm), Streams, & Pirus

The first major distributed denial of service attacks shut down major sites such as Yahoo!, Amazon.com, and others. In May the Love Letter worm became the fastest-spreading worm (to that time); shutting down E-mail systems around the world. June 2000 saw the first attack against a telephone system. The Visual Basic Script worm Timofonica tries to send messages to Internet-enabled phones in the Spanish telephone network (later in 2000 another Trojan attacked the Japanese emergency phone system). August 2000 saw the first Trojan developed for the Palm PDA. Called Liberty and developed by Aaron Ardiri the co-developer of the Palm Game Boy emulator Liberty, the Trojan was developed as an uninstall program and was distributed to a few people to help foil those who would steal the actual software. When it was accidentally released to the wider public Ardiri helped contain its spread. Streams became the first proof of concept NTFS Alternate Data Stream (ADS) virus in early September. As a proof of concept, Streams has not circulated in the wild (as of this writing) but as in all such cases a circulating virus based on the model is expected. Pirus is another proof of concept for malware written in the PHP scripting language. It attempts to add itself to HTML or PHP files. Pirus was discovered 9 Nov 2000.

2001 - Gnuman, Winux Windows/Linux Virus, LogoLogic-A

Worm, ApIS/Simpsons Worm, PeachyPDF-A, Nimda

Gnuman (Mandragore) showed up the end of February. This worm cloaked itself from the Gnutella file-sharing system (the first to specifically attack a peer-to-peer communications system) and pretended to be an MP3 file to download. In March a proof of concept virus designed to infect both Windows and Linux (and cross between them) was released. Winux (or Lindose depending on who you talk to) is buggy and reported to have come from the Czech Republic. On 9 April a proof of concept Logo Worm was released for the SuperLogo language by Logotron. LogoLogic-A spreads via MIRC chat and E-mail. May saw the first AppleScript worm. It uses Outlook Express or Entourage on the Macintosh to spread via E-mail to address book entries. Early August, the PeachyPDF-A worm became the first to spread using Adobe's PDF software. Only the full version, not the free PDF reader, was capable of spreading the worm so it did not go far. September, the [Nimda](#) worm demonstrated significant flexibility in its ability to spread and used several firsts. While not new in concept, a couple of worms created a fair amount of havoc during the year: Sircam (July), CodeRed (July & August), and BadTrans (November & December).

2002 - LFM-926, Donut, Sharp-A, SQLSpider, Benjamin, Perrun

Early in January LFM-926 showed up as the first virus to infect Shockwave Flash (.SWF) files. It was named for the message it displays while it's infecting: "Loading.Flash.Movie…". It drops a Debug script that produces a .COM file which infects other .SWF files. Also in early January Donut showed up as the first worm directed at .NET services. In March, the first native .NET worm written in C#, Sharp-A was announced. Sharp-A was also unique in that it was one of the few malware programs reportedly written by a woman. Late May the Javascript worm SQLSpider was released. It was unique in that it attacked installations running Microsoft SQL Server (and programs

that use SQL Server technology). Also in late May the Benjamin appeared. Benjamin is unique in that it uses the KaZaa peer-to-peer network to spread. Mid-June the press went wild over the proof-of-concept Perrun virus because a portion of the virus attached itself to JPEG image files. Despite the hype, JPEG files are still safe as you must have a stripper program running on your system in order to strip the virus file off the image file.

Your choice from here; read some detailed histories of the early years or move on to Virus Protection techniques.

[Dr. Solomon's History](#)…

[Robert M. Slade's History](#)…

[Virus Protection](#)…

Please visit our sponsors.

[Click Here to Visit our Sponsor](#)

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.

cknow.com

Virus Tutorial

Navigation

Virus Protection

Tutorial Map

Anti-Virus Software

Virus Protection

Finding a virus on your system may not be easy; they often don't cooperate. Using anti-virus tools is important.

A virus may or may not present itself. Viruses attempt to spread before activating whatever malicious activity they may have been programmed to deliver. So, viruses will often try to hide themselves. Sometimes there are symptoms that can be observed by a trained casual observer who knows what to look for (but, don't count on it).

Virus authors often place a wide variety of indicators into their viruses (e.g., messages, music, graphic displays). These, however, typically only show up when the virus payload activates. With DOS systems, the unaccounted for reduction of the amount of RAM known to be in the computer is an important indicator resident viruses have a hard time getting around. But, under Windows, there is no clear indicator like that. The bottom line is that one must use anti-virus software to detect (and fix) most viruses.

Your main defense is to detect and identify specific virus attacks to your computer. There are three methods in

general use. Each has pros and cons and are discussed via these links. Often, a given anti-virus software program will use some combination of the three techniques for maximum possibility of detection.

- [Scanning](#)
- [Integrity Checking](#)
- [Interception](#)

In a more general sense, check here for some ideas about using the above-referenced methods and other useful information:

- [AV Product Use Guidelines](#)
- [File Extensions](#)
- [Safe Computing Practices (Safe Hex)](#)
- [Outlook and Outlook Express](#)
- [Disable Scripting](#)
- [Backup Strategy](#)

Another line of defense is continuing education. Click below to see some sources of on-going information.

- [On-going Virus Information](#)

Summary

- Viruses, by design, are hard to find using standard tools. SCANDISK and MEM can help, but don't rely on them to find viruses and never rely on DOS commands to eliminate a virus.
- Anti-virus software helps using techniques of:
  - Scanning
  - Interception
  - Integrity Checking
- You can help by taking some common sense precautions and keeping educated.

Now, let's look at scanning…

Please visit our sponsors.

Click Here to Visit our Sponsor

Protection Intro | Scanning | Integrity Checking | Interception | AV Product Use | File Extensions | Safe Hex | Outlook vs. Outlook Express | Scripting | Backup | On-going Virus Info
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Virus Tutorial

Virus Hoaxes

Virus Hoaxes

Virus myths abound. Hoaxes are easy to construct and also freely circulate. Learn about them.

Navigation

Tutorial Map

Anti-Virus Software

Viruses, by their nature, tend to mystify the average user. They operate in the background under rules that are little understood by most users. As such, a mythology has developed where stories are passed from person to person as true; yet few are based in fact.

Most hoaxes, while deliberately posted, die a quick death because of their outrageous content. Some, however, make it into the wild and get out of hand.

A lot of hoaxes spout some pretty good technobabble, so unless you are a real expert, it's easy to get caught. Look for specific technical details, particularly how to identify and get rid of the beast. If you don't recognize the name of the person posting the warning, check to see who they say they have sent copies to for study. Independently verify the report with secondary sources.

Before jumping into the deep end of the pool and believing everything that comes across the net, check it out:

- Look at the location of the posting. If the posting is in an inappropriate newsgroup be suspicious.
- Look at the poster. Is it someone who is clearly identified and is a known expert on the subject of the posting?
- Look closely at the details:
  - If it involves government action there should be some reference to an easily-obtained bill or federal regulation.
  - If it involves something technical look for obvious technobabble (e.g., Nth complexity infinite binary loop).
  - Double check it anyhow!

You can research hoaxes at some of the resources listed here:

- If you suspect a virus hoax, Computer Knowledge's favorite site is: http://www.vmyths.com/ (this site is run by a friend; it doesn't affect the recommendation but you should know that in advance for full disclosure purposes--see the False Authority Syndrome discussion for reasons why). If you can't find a reference at vmyths.com they have links to other relevant sites.

Some interesting urban legend sites to check are:

- Urban Legends and Folklore
- Urban Legends Reference
- CIAC Internet Hoaxes

And, finally, most anti-virus sites have a section on their web site that discusses the most current hoaxes.

Quick and Easy Cures

The simple point to make here is: **there are none**. Any product that advertises itself as a "quick and easy cure" for

"all viruses past, present, and future" is more likely than not exercising its advertising imagination. Everyone would like to just buy product X, run it, and be rid of viruses forever. Unfortunately **there is no such easy cure**.

Of course, this tutorial is only a broad-brush introduction to the topic. If you want to keep up with hoaxes and myths as they spread around the world take a look at the resources above.

Summary

- Being largely misunderstood, viruses easily generate myths.
- Some people think it's funny to generate hoaxes. By careful checking you can usually spot them.
- Silly tricks and poor policies are no substitute for individual protection methods.

Please visit our sponsors.

Click Here to Visit our Sponsor

Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

ckrow.com

Virus Tutorial

Current Threats

Summaries of current threats are linked to this page.

Navigation

Current Threats

Tutorial Map

Anti-Virus Software

Below are links to pages that describe some of the more common viruses and worms. These are presented more for their educational value as to what these beasts can do and (basically) how they do it. This is **NOT** a tutorial on how to write a virus, nor is it designed to be the quickest source of information about the latest virus/worm getting exposure in the press.

If you don't see the virus/worm you are looking for here please visit one of the anti-virus vendor sites and check their much more complete and up-to-date encyclopedias. Also, brief summaries of new viruses are placed into the Computer Knowledge monthly newsletter.

Here we have profiles for…

- **Back Orifice**
  A backdoor Trojan.
- **CIH Spacefiller**
  A file-infecting virus the press dubbed Chernobyl.

- **Kakworm**
  Worm that exploits security vulnerabilities in IE and Outlook.
- **Laroux**
  The most widespread Excel macro virus.
- **Love Letter**
  Worm that sends itself as an attachment to E-mail.
- **Melissa**
  The original widespread E-mail worm.
- **Nimda**
  A worm with many infection techniques.
- **Pretty Park**
  Trojan that can serve as a backdoor into your computer.
- **Stages**
  An E-mail worm that is believed to be the first use of a scrap file to spread.

Current Threats | Back Orifice | CIH Spacefiller | Kakworm | Laroux | Love Letter | Melissa | Nimda | Pretty Park | Stages
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

ckNOW.com

Virus Tutorial

Navigation

Virus Intro

Tutorial Map

Anti-Virus Software

Virus Behavior

Viruses come in a great many different forms, but they all potentially have two phases to their execution, the infection phase and the attack phase:

Infection Phase

> **Virus writers have to balance how and when their viruses infect against the possibility of being detected. Therefore, the spread of an infection may not be immediate.**

When the virus executes it has the potential to infect other programs. What's often not clearly understood is precisely when it will infect the other programs. Some viruses infect other programs each time they are executed; other viruses infect only upon a certain trigger. This trigger could be anything; a day or time, an external event on your PC, a counter within the virus, etc. Virus writers want their programs to spread as far as possible before anyone notices them.

It is a serious mistake to execute a program a few times -

find nothing infected and presume there are no viruses in the program. You can never be sure the virus simply hasn't yet triggered its infection phase!

Many viruses go resident in the memory of your PC in the same or similar way as terminate and stay resident (TSR) programs. (For those not old enough to remember TSRs, they were programs that executed under DOS but stayed in memory instead of ending.) This means the virus can wait for some external event before it infects additional programs. The virus may silently lurk in memory waiting for you to access a diskette, copy a file, or execute a program, before it infects anything. This makes viruses more difficult to analyze since it's hard to guess what trigger condition they use for their infection.

On older systems, standard (640K) memory is not the only memory vulnerable to viruses. It is possible to construct a virus which will locate itself in upper memory (the space between 640K and 1M) or in the High Memory Area (the small space between 1024K and 1088K). And, under Windows, a virus can effectively reside in **any** part of memory.

Resident viruses frequently take over portions of the system software on the PC to hide their existence. This technique is called stealth. Polymorphic techniques also help viruses to infect yet avoid detection.

Note that worms often take the opposite approach and spread as fast as possible. While this makes their detection virtually certain, it also has the effect of bringing down networks and denying access; one of the goals of many worms.

Attack Phase

> # Viruses need time to infect. Not all viruses attack, but all use system resources and often have bugs.

Many viruses do unpleasant things such as deleting files or changing random data on your disk, simulating typos or merely slowing your PC down; some viruses do less harmful things such as playing music or creating messages or animation on your screen. Just as the infection phase can be triggered by some event, the attack phase also has its own trigger.

Does this mean a virus without an attack phase is benign? No. Most viruses have bugs in them and these bugs often cause unintended negative side effects. In addition, even if the virus is perfect, it still steals system resources. (Also, see the "good" virus discussion.)

Viruses often delay revealing their presence by launching their attack only after they have had ample opportunity to spread. This means the attack could be delayed for days, weeks, months, or even years after the initial infection.

The attack phase is optional, many viruses simply reproduce and have no trigger for an attack phase. Does this mean that these are "good" viruses? No! Anything that writes itself to your disk without your permission is stealing storage and CPU cycles. (Also see the "good" virus discussion.) This is made worse since viruses that "just infect," with no attack phase, often damage the programs or disks they infect. This is not an intentional act of the virus, but simply a result of the fact that many viruses contain extremely poor quality code.

An an example, one of the most common past viruses, Stoned, is not intentionally harmful. Unfortunately, the author did not anticipate the use of anything other than 360K floppy disks. The original virus tried to hide its own

code in an area of 1.2MB diskettes that resulted in corruption of the entire diskette (this bug was fixed in later versions of the virus).

Number of Viruses…

Please visit our sponsors.

Click Here to Visit our Sponsor

Behaviour | Number | Names | How Serious? | Good Viruses? | Hardware Threats | Software Threats
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Virus Tutorial

Navigation

Virus Intro

Tutorial Map

Anti-Virus Software

Number of Viruses

There are currently over 50,000 computer viruses and that number is growing rapidly. Fortunately, only a small percentage of these are circulating widely.

There are more MS-DOS/Windows viruses than all other types of viruses combined (by a large margin). Estimates of exactly how many there are vary widely and the number is constantly growing.

In 1990, estimates ranged from 200 to 500; then in 1991 estimates ranged from 600 to 1,000 different viruses. In late 1992, estimates were ranging from 1,000 to 2,300 viruses. In mid-1994, the numbers vary from 4,500 to over 7,500 viruses. In 1996 the number climbed over 10,000. 1998 saw 20,000 and 2000 topped 50,000. It's easy to say there are more now.

The confusion exists partly because it's difficult to agree on how to count viruses. New viruses frequently arise from someone taking an existing virus that does something like put a message out on your screen saying: "Your PC is now stoned" and changing it to say something like "Donald Duck is

a lie!". Is this a new virus? Most experts say yes. But, this is a trivial change that can be done in less than two minutes resulting in yet another "new" virus.

Another problem comes from viruses that try to conceal themselves from scanners by mutating. In other words, every time the virus infects another file, it will try to use a different version of itself. These viruses are known as polymorphic viruses.

One example, the Whale (a huge clumsy 10,000 byte virus), creates 33 different versions of itself when it infects files. At least one person counts this as 33 different viruses on their list. Many of the large number of viruses known to exist have not been detected in the wild but probably exist only in someone's virus collection.

David M. Chess of IBM's High Integrity Computing Laboratory reported in the November 1991 Virus Bulletin that "about 30 different viruses and variants account for nearly all of the actual infections that we see in day-to-day operation." Now, about 180 different viruses (and some of these are members of a single family) account for all the viruses that actually spread in the wild. To keep track visit the Wildlist, a list which reports virus sightings.

How can there be so few viruses active when some experts report such high numbers? This is probably because most viruses are poorly written and cannot spread at all or cannot spread without betraying their presence. Although the actual number of viruses will probably continue to be hotly debated, what is clear is that the total number of viruses is increasing, although the active viruses not quite as rapidly as the numbers might suggest.

Summary

- By number, there are over 50,000 known computer viruses.

- Only a small percentage of this total number account for those viruses found in the wild, however. Most exist only in collections.

How are viruses named?… Next

Please visit our sponsors.

Click Here to Visit our Sponsor

Behaviour | Number | Names | How Serious? | Good Viruses? | Hardware Threats | Software Threats
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

ckmow.com

Virus Tutorial

Virus Names

Navigation

Virus Intro

Tutorial Map

Anti-Virus Software

Virus Names

> A virus' name is generally assigned by the first researcher to encounter the beast. The problem is that multiple researchers may encounter a new virus in parallel which often results in multiple names.

What's in a name? When it comes to viruses it's a matter of identification to the general public. An anti-virus program does not really need the name of a virus as it identifies it by its characteristics. But, while giving a virus a name helps the public at large it also serves to confuse them since the names given to a particular beast can differ from anti-virus maker to anti-virus maker.

How? Why? Much as they would like to, the virus writers do not get to name their beasts. Some have tried by putting obvious text into the virus but most of the anti-virus companies tend to ignore such text (mostly to spite the virus writers 😎). And, any virus writer that insists on a particular name has to identify themselves in the process--something they usually don't want to do. So, the anti-virus companies control the virus naming process. But, that leads to the

naming problem.

Viruses come into various anti-virus companies around the world at various times and by various means. Each company analyzes the virus and assigns a name to it for tracking purposes. While there is cooperation between companies when new viruses are identified, that cooperation often takes a back seat to getting a product update out the door so the anti-virus company's customers are protected. This delay allows alternate names to enter the market. Over time these are often standardized or, at least, cross-referenced in listings; but that does not help when the beast makes its first appearance.

This problem/confusion will continue. One practical and well documented example of how it affects a real-world virus listing can be seen at the WildList site on the page…

http://www.wildlist.org/naming.htm

One attempt at bringing some order to the naming problem is Ian Whalley's VGrep. VGrep attempts to collect all of the various virus names and then correlates them into a single searchable list. While useful, there is, again, the lag time necessary to collect and correlate the data.

So, get used to viruses having different names. As Shakespeare said…

What's in a name? That which we call a rose
By any other name would smell as sweet…

Summary

- Virus naming is a function of the anti-virus companies. This results in different names for new viruses.
- Different names can cause confusion for the public but not anti-virus software which looks at the virus, not its "name."

- There are different sites that attempt to correlate the various virus names for you.

How serious are viruses?…

Behaviour | Number | Names | How Serious? | Good Viruses? | Hardware Threats | Software Threats
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

---

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Virus Introduction

Virus Tutorial

Navigation

Virus Intro

Tutorial Map

Anti-Virus Software

How Serious Are Viruses?

> While serious if you have one, viruses are only one way your data can be damaged. You must be prepared for all threats; many of which are more likely to strike than viruses.

It's important to keep viruses in perspective. There are many other threats to your programs and data that are much more likely to harm you than viruses. A well known anti-virus researcher once said that you have more to fear from a cup of coffee (which may spill) than from viruses. While the growth in number of viruses and introduction of the Microsoft Word® macro viruses and VisualBasic Script worms now puts this statement into question (even though you can avoid these by just not clicking on them to open them!), it's still clear that there are many dangerous occurrences of data corruption from causes other than from viruses.

So, does this mean that viruses are nothing to worry about? **Emphatically, no!** It just means that it's foolish to spend much money and time on addressing the threat of viruses if you've done nothing about the other more likely threats to your files. Because viruses and worms are deliberately written to invade and possibly damage your PC, they are the

most difficult threat to guard against. It's pretty easy to understand the threat that disk failure represents and what to do about it (although surprisingly few people even address this threat). The threat of viruses is much more difficult to deal with. There are no "cures" for the virus problem. One just has to take protective steps with anti-virus software and use some common sense when dealing with unknown files.

Summary

- While viruses are a serious threat, there are other, probably more serious, threats to your data.
- If you have not taken precautions (e.g., regular backup) against general threats you have not properly protected your computer.

[What about a good virus?](#)... **Next**

Please visit our sponsors.

Click Here to Visit our Sponsor

Behaviour | Number | Names | How Serious? | Good Viruses? | Hardware Threats | Software Threats
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
[Pray the Rosary](#) for peace.

cknow.com

Virus Introduction

Virus Tutorial

What About Good Viruses?

Navigation

Virus Intro

Tutorial Map

Anti-Virus Software

The general consensus is that there are none.

By definition, viruses do not have to do something bad. An early (and current) virus researcher, Fred Cohen, has argued that good computer viruses are a serious possibility. In fact, he has offered a reward of $1,000 for the first clearly useful virus; but, he hasn't paid yet.

Most researchers, however, take the other side and argue that the use of self-replicating programs are never necessary; the task that needs to be performed can just as easily be done without the replication function.

Vesselin Bontchev has written a paper originally delivered at the 1994 EICAR conference, titled *Are "Good" Computer Viruses Still a Bad Idea?*. The paper covers all aspects of the topic. As of this writing, the paper is available at:

ftp://ftp.informatik.uni-hamburg.de/pub/virus/texts/viruses/goodvir.zip

Lest you think others have not been thinking about this,

here are some of the proposals (from the above-referenced paper) for a good virus that have not worked out:

- **The "Anti-Virus" Virus.** Several people have had the idea to develop an "anti-virus" virus - a virus which would be able to locate other (presumably malicious) computer viruses and remove them.
- **The "File Compressor" Virus.** This is one of the oldest ideas for "beneficial" viruses. The idea consists of creating a self-replicating program, which will compress the files it infects, before attaching itself to them.
- **The "Disk Encryptor" Virus.** This virus has been published. The idea is to write a boot sector virus, which encrypts the disks it infects with a strong encryption algorithm (IDEA in this particular case) and a user-supplied password to ensure the privacy of the user's data.
- **The "Maintenance" Virus.** The idea consists of a self-contained program, which spawns copies of itself across the different machines in a network (thus acting more like a worm) and performing some maintenance tasks on those machines (like deleting temporary files).

All of the above viruses fail one or more of the standard measures typically used to judge if a virus is "good" or not. These are (again, from the above-referenced paper):

- **Technical Reasons**
  - **Lack of Control.** Once released, the person who has released a computer virus has no control on how this virus will spread.
  - **Recognition Difficulty.** In general it is not always possible to distinguish between a virus and a non-virus program. There is no reason to think that distinguishing between "good" and "bad" viruses will be much easier. Many people are relying on generic anti-virus defenses (e.g., activity monitoring and/or integrity checking)

which will trigger a response to changes.

- ○ **Resource Wasting.** A computer virus eats up disk space, CPU time, and memory resources during its replication.
- ○ **Bug Containment.** A computer virus can easily escape a controlled environment.
- ○ **Compatibility Problems.** A computer virus that attaches itself to user programs would disable several programs on the market that perform a checksum on themselves at runtime.

- **Ethical and Legal Reasons**
  - ○ **Unauthorized Data Modification.** It is usually considered unethical to modify other people's data without their authorization. In many countries this is also illegal.
  - ○ **Copyright and Ownership Problems.** In many cases, modifying a particular program could mean that copyright, ownership, or at least technical support rights for this program are voided.
  - ○ **Possible Misuse.** An attacker could use a "good" virus as a means of transportation to penetrate a system.
  - ○ **Responsibility.** Declaring some viruses as "good" and "beneficial" would just provide an excuse to the crowd of irresponsible virus writers to condone their activities and to claim that they are actually doing some kind of "research."

- **Psychological Reasons**
  - ○ **Trust Problems.** Users like to think that they have full control on what is happening in their machine.
  - ○ **Negative Common Meaning.** For most people, the word "computer virus" is already loaded with negative meaning.

Summary

While frequently discussed, the general consensus is that there is no task that requires a

virus.

[Hardware Threats](#)...

Behaviour | Number | Names | How Serious? | Good Viruses? | Hardware Threats | Software Threats
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

---

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Virus Tutorial

Navigation

Virus Intro

[Tutorial Map](#)

[Anti-Virus Software](#)

Hardware Threats

> Hardware is a common cause of data problems. Power can fail, electronics age, add-in boards can be installed wrong, you can mistype, there are accidents of all kinds, a repair technician can actually cause problems, and magnets you don't know are there can damage disks.

Hardware problems are all too common. We all know that when a PC or disk gets old, it might start acting erratically and damage some data before it totally dies. Unfortunately, hardware errors frequently damage data on even young PCs and disks. Here are some examples.

Power Faults

Your PC is busy writing data to the disk and the lights go out! "Arghhhh!" Is everything OK? Maybe so, maybe not; it's vital to know for sure if anything was damaged.

Other power problems of a similar nature would include brownouts, voltage spikes, and frequency shifts. All can

cause data problems, particularly if they occur when data is being written to disk (data in memory generally does not get corrupted by power problems; it just gets erased if the problems are serious enough).

- **Brownout:** Lower voltages at electrical outlets. Usually they are caused by an extraordinary drain on the power system. Frequently you will see a brownout during a heat wave when more people than normal have air conditioners on full. Sometimes these power shortages will be "rolling" across the area giving everyone a temporary brownout. Maybe you'll get yours just as that important file is being written to disk.
- **Voltage Spikes:** Temporary voltage increases are fairly common. Large motors or circuit breakers in industry can put them on the electrical line. Sudden losses (e.g., a driver hits a power pole) can causes spikes as the circuits balance. An appliance in your home can cause a spike, particularly with older wiring. Lightning can put large spikes on power lines. And, the list goes on. In addition to current backups and integrity information for your software and data files, including a hardware voltage spike protection device between the wall and your computer hardware (don't forget the printer and monitor) can be very helpful.
- **Frequency Shifts:** While infrequent, if the line frequency varies from the normal 60 Hertz (or 50 Hertz in some countries), the power supply on the computer can be affected and this, in turn, can reflect back into the computer causing data loss.

Age

It's not magic; as computers age they tend to fail more often. Electronic components are stressed over time as they heat up and cool down. Mechanical components simply wear out. Some of these failures will be dramatic; something will just stop working. Some, however, can be slow and not obvious. Regrettably, it's not a question of "if", but "when" in

regard to equipment failure.

Incompatibilities

You can have hardware problems on a perfectly healthy PC if you have devices installed that do not properly share interrupts. Sometimes problems are immediately obvious, other times they are subtle and depend upon certain events to happen at just the wrong time, then suddenly strange things happen! (Software can do this too!)

Finger Faults

(Typos and "OOPS! I didn't mean to do that!")

These are an all too frequent cause of data corruption. This commonly happens when you are intending to delete or replace one file but actually get another. By using wild cards, you may experience a really "wild" time. "Hmmm I thought I deleted all the *.BAK files; but they're still here; something was deleted; what was it? Or was I in the other directory?" Of course if you're a programmer or if you use sophisticated tools like a sector editor, then your fingers can really get you into trouble!

Malicious or Careless Damage

Someone may accidentally or deliberately delete or change a file on your PC when you're not around. If you don't keep your PC locked in a safe, then this is a risk. Who knows what was changed or deleted? Wouldn't it be nice to know if anything changed over the weekend? Most of this type of damage is done unintentionally by someone you probably know. This person didn't mean to cause trouble; they simply didn't know what they were doing when they used your PC.

Typhoid Mary

One major source for computer infections is the Customer Engineer (CE), or repairman. When a CE comes for a service call, they will almost always run a diagnostic program from diskette. It's very easy for these diskettes to become infected and spread the infection to your computer. Sales representatives showing demonstrations via floppy disks are also possibly spreading viruses. Always check your system after other people have placed their floppy disk into it. (Better yet, if you can, check their disk with up-to-date anti-virus software **before** anything is run.)

Magnetic Zaps

Computer data is generally stored as a series of magnetic changes on disks. While hard disks are generally safe from most magnetic threats because they are encased within the computer compartment, floppy disks are highly vulnerable to magnets. The obvious threat would be to post a floppy disk to the refrigerator with a magnet; but there are many other, more subtle, threats.

Some of the more subtle sources of magnetism include:

- **Computer Monitor**. Don't put floppy disks anywhere near the monitor; it generates a magnetic field.
- **Telephone**. When ringing, telephones (particularly older phones with a bell) generate a magnetic field.
- **Bottom Desk Drawer**. While the desk drawer does not generate a magnetic field, the vacuum cleaner that the maintenance people slide under the desk to clean the floor does.
- **Bottom Bookcase Shelf and File Cabinet Drawer**. Same comment as the desk drawer just above.
- **Pets**. Pet fur generates a strong electrostatic charge which, if discharged through a disk, can affect files on the disk. Instead of "The dog ate my homework," today it could just as easily be: "The cat sat on my homework."

Bottom line: There are tools to assist in recovery from disk

problems, but how do you know all the data is OK? These tools do not always recover good copies of the original files. Active action on your part before disaster strikes is your best defense. It's best to have a good, current backup and, for better protection, a complete up-to-date integrity-check map of everything on your disk.

Summary

- There are many different kinds of hardware threats to your data. Some include:
  - Power faults
  - Age
  - Equipment incompatibilities
  - Typos
  - Accidental or deliberate damage
  - The Customer Engineer or friendly salesperson
  - Problems with magnets
- Active action on your part can help you identify problems and, perhaps, head them off early.

Software Threats…

Please visit our sponsors.

Click Here to Visit our Sponsor

Behaviour | Number | Names | How Serious? | Good Viruses? | Hardware Threats | Software Threats
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Send mail to webmaster@cknow.com with questions or comments about this web site.

Copyright © 2001 Computer Knowledge, All Rights Reserved

[Pray the Rosary](#) for peace.

ckcnow.com

Virus Introduction

Virus Tutorial

Click Here to Visit our Sponsor

Navigation

Virus Intro

Tutorial Map

Anti-Virus Software

Software Threats

> **Software interactions are a significant source of problems; but these are inadvertent. Software attacks are deliberate and can also be significant.**

Software threats can be general problems or an attack by one or more types of malicious programs.

Software Problems

This category accounts for more damage to programs and data than any other. We're talking about non-malicious software problems here, not viruses. Software conflicts, by themselves, are much more likely threats to your PC than virus attacks.

We run our PCs today in a complex environment. There are many resident programs (e.g., anti-virus, video drivers) running simultaneously with various versions of Windows, DOS, BIOS, and device drivers. All these programs execute at the same time, share data, and are vulnerable to unforeseen interactions between each other. Naturally, this means that there may be some subtle bugs waiting to "byte" us. Any

time a program goes haywire, there's the risk it may damage information on disk.

There's the further problem that not all programs do what we hope they will. If you have just undeleted a file, you don't really know if all the correct clusters were placed back in the right order. When SCANDISK "fixes" your disk for you, you have no way of knowing exactly what files it changed to do its job. It becomes even more complex if you use other utilities to do similar tasks.

Software problems happen and can be very serious if you have not taken appropriate action in advance of the problem.

Software Attacks

These are programs written deliberately to vandalize someone's computer or to use that computer in an unauthorized way. There are many forms of malicious software; sometimes the media refers to all malicious software as viruses. This is not correct and it's important to understand the distinction between the various types as it has some bearing on how you react to the attack. The discussions that follow attempt to make clear distinctions between malicious software types. Realize that often a malicious program may have characteristics of more than one of these types (e.g., a virus that attacks files but also spreads itself across a network). Don't get wrapped up in the semantics, just try to understand the major differences.

In addition to viruses, the main thrust of this tutorial, there are:

- Logic Bombs. Just like a real bomb, a logic bomb will lie dormant until triggered by some event.
- Trojans. These are named after the Trojan horse, which delivered soldiers into the city of Troy.
- Worms. A worm is a self-reproducing program that

does not infect other programs as a virus will, but instead creates copies of itself, that create even more copies.

Summary

- Non-malicious software problems can be a significant source of problems and one should always know their computer's exact configuration to be prepared.
- Malicious software falls into several general categories:
  ○ Logic bombs
  ○ Trojans
  ○ Worms
  ○ Viruses

That's the end of the introduction. Now for the detail…

Virus Types…

Behaviour | Number | Names | How Serious? | Good Viruses? | Hardware Threats | Software Threats
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.

[Pray the Rosary](#) for peace.

CKNOW.COM

Virus Tutorial

Navigation

Virus Types

Tutorial Map

Anti-Virus Software

What Viruses Infect

Viruses can infect a number of different portions of the computer's operating and file system. These include:

- **System Sector Viruses**
  These infect control information on the disk itself.
- **File Viruses**
  These infect program (COM and EXE) files.
- **Macro Viruses**
  These infect files you might think of as data files. But, because they contain macro programs they can be infected.
- **Companion Viruses**
  A special type that adds files that run first to your disk.
- **Cluster Viruses**
  A special type that infects through the disk directory.
- **Batch File Viruses**
  These use text batch files to infect.
- **Source Code Viruses**
  These add code to actual program source code.
- **Visual Basic Worms**
  These worms use the Visual Basic language to control the computer and perform tasks.

Please visit our sponsors.

Click Here to Visit our Sponsor

What Viruses Infect | | | System Sector | File | Macro | Companion | Cluster | Batch File | Source Code | Visual Basic Worms
How Viruses Infect | | | Polymorphic | Stealth | Fast and Slow | Sparse | Armored | Multipartite | Spacefiller | Tunneling |
Camouflage | NTFS ADS | Virus Droppers
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Virus Tutorial

Navigation

Virus Types

Tutorial Map

Anti-Virus Software

System Sector Viruses

> System sectors (Master Boot Record and DOS Boot Record) are often targets for viruses. These boot viruses use all of the common viral techniques to infect and hide themselves. While mostly obtained from an infected disk left in the drive when the computer starts, they can also be "dropped" by some file infectors.

System sectors are special areas on your disk containing programs that are executed when you boot (start) your PC. Every disk (even if it only contains data) has a system sector of some sort. Sectors are simply small areas on your disk that your hardware reads in single chunks. System sectors are invisible to normal programs but are vital for correct operation of your PC. They are a common target for viruses. There are two types of system sectors found on DOS/Windows PCs:

- **DOS Boot Sectors** (DBS)
- **Partition Sectors** (often called Master Boot Record or MBR)

System sector viruses modify the program in either the DOS boot sector or the Master Boot Record. Since there isn't much room in the system sector (only 512 bytes), these viruses usually have to hide their code somewhere else on the disk. These viruses sometimes cause problems when this spot already contains data that is then overwritten.

Some viruses, such as the Pakistani Brain virus, mark the spot where they hide their code as bad. This is one reason to be suspicious if any utility suddenly reports additional bad sectors on your disk and you don't know why (don't panic, bad sectors occur frequently for a wide variety of reasons). These viruses usually go resident in memory on your PC, infect the hard disk, and infect any floppy disk that you access. Simply looking at the directory of a floppy disk may cause it to be infected if one of these viruses is active in memory.

On Macintosh systems, some viruses will even infect a diskette immediately upon inserting a diskette into the floppy drive. (PCs generally do not access a disk automatically as the Macintosh does.)

Since viruses are active in memory (resident), they can hide their presence. If Brain is active on your PC, and you use a sector editor to look at the boot sector of an infected diskette, the virus will intercept the attempt to read the infected boot sector and instead return a saved image of the original boot sector. You will see the normal boot sector instead of the infected version. Viruses that do this are known as stealth viruses.

In addition to infecting diskettes, some system sector viruses also spread by infecting files. Viruses of this type are called multipartite (multiple part) viruses. Since they can infect both files and system sectors they have more avenues to spread. (**Note:** Some file viruses also infect system sectors to complete the circle.)

Summary

- System sectors (MBR and DBS) are often targets for viruses.
- Even data disks can be infected by these viruses.
- System sector viruses spread easily via floppy disk infections and, in some cases, by cross infecting files which then drop system sector viruses when run on clean computers.

File Viruses…

What Viruses Infect | | | System Sector | File | Macro | Companion | Cluster | Batch File | Source Code | Visual Basic Worms
How Viruses Infect | | | Polymorphic | Stealth | Fast and Slow | Sparse | Armored | Multipartite | Spacefiller | Tunneling |
Camouflage | NTFS ADS | Virus Droppers
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.

Pray the Rosary for peace.

ckNOW.COM

Virus Tutorial

Virus Types/Methods

Navigation

Virus Types

Tutorial Map

Anti-Virus Software

File Viruses

> While more in number, file infectors are not the most commonly found. They infect in a variety of ways and can be found in a large number of file types.

In terms of sheer number of viruses, these were the most numerous for some time. However, because of bugs in the virus code, they are not the most widely spread. Macro viruses (and system sector viruses) account for more infections in the wild and macro viruses themselves have probably overtaken file viruses in sheer numbers by now.

The simplest file viruses work by locating a type of file they know how to infect (usually a file name ending in .COM or .EXE) and overwriting part of the program they are infecting. When this program is executed, the virus code executes and infects more files. These overwriting viruses do not tend to be very successful since the overwritten program rarely continues to function correctly and the virus is almost immediately discovered.

The more sophisticated file viruses save (rather than overwrite) the original instructions when they insert their code into the program. This allows them to execute the

original program after the virus finishes so that everything appears normal.

Just as system sector viruses can remain resident in memory and use stealth techniques to hide their presence, file viruses can also hide this way. If you do a directory listing, you will not see any increase in the length of the file and if you attempt to read the file, the virus will intercept the request and return your original uninfected program to you.

Some file viruses (such as 4096) also infect overlay files as well as the more usual *.COM and *.EXE files. Overlay files have various extensions, but .OVR and .OVL are common. Files with the extension .DLL are also capable of being infected (but generally are not; typically they are only libraries of functions). Indeed, as operating systems become more advanced, typically more files become able to contain executable code and thus be vulnerable to infection. (See the file extension list for a more complete summary.)

Summary

- File viruses number in the thousands, but are not the most widely found in the wild.
- File viruses have a wide variety of infection techniques and infect a large number of file types.

Macro Viruses…

What Viruses Infect | | | System Sector | File | Macro | Companion | Cluster | Batch File | Source Code | Visual Basic Worms
How Viruses Infect | | | Polymorphic | Stealth | Fast and Slow | Sparse | Armored | Multipartite | Spacefiller | Tunneling |
Camouflage | NTFS ADS | Virus Droppers
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Virus Tutorial

Please visit our sponsors.

Click Here to Visit our Sponsor

Navigation

Virus Types

Tutorial Map

Anti-Virus Software

Macro Viruses

> Pure data files cannot propagate viruses, but with extensive macro languages in some programs the line between a "data" file and executable file can easily become blurred to the average user. While text E-mail messages can't contain viruses they may have attachments that do and some E-mail programs will automatically load and run these. Don't let them. Finally, be careful of programs that use other programs for reading E-mail.

As indicated throughout this tutorial, in order for a virus to do anything, first a program of some type must execute. A virus, no matter what type, is still a program and it must load into memory and run in order to do anything. Simply reading it into memory is not sufficient. Pure data files are not viruses simply because, by their nature, they do not execute.

The problem, however, is that many modern programs contain some form of macro language; in some cases a very powerful macro language with commands that include

opening, manipulating, and closing files. More and more, these programs allow a user to extend their capabilities by writing powerful macros and then attaching these to data files produced by that program. In many cases, in order to make things easy for users, the macros are set up to run automatically whenever the data file is loaded. It's in cases like this where the line between a data file and program starts to blur.

Note: There are many triggers (other than loading the document) that viral code can exploit. And, once running, various elements of the program's macro language can be exploited so that all future data files produced by that program version could contain the viral macro code.

Most scanners have default settings that check the most common executable files and data files from programs that have a macro language. So, when using those programs it's a good idea to not change the default extension so scanners can find the files they need to. Also, scanners can be set to check every file instead of just files that normally execute; but most do not do this by default--that would make the scanning process too long for most people.

In order to know when to turn full scanning on you need to know something about the software you use. In particular, you need to make yourself aware of any software that uses the sort of "automatic macro" feature described here. Never use a piece of software until you've explored its manual for some time just to see its full capabilities. If these include some sort of "programming" (macro) language, be aware there is an opportunity for problems. Common programs with macro capability that can be exploited by virus writers are Microsoft Word®, Excel® and other Office programs. Windows Help files can also contain macro code (but are rarely exploited because of the difficulty in doing so). And, the latest macro code to be exploited exists in the full version of the Acrobat program which reads and writes PDF files (the free reader is **not** affected; only the full version).

A second vulnerability exists on the Internet. Some E-mail programs and Internet browsers allow you to click on a data file or program that might be attached to a message or displayed on a web page and have that file or program load and/or run automatically. **You should not allow this to happen.** Always save the file or program to disk and then check it with anti-virus software before loading or executing it (or have an anti-virus program that "attaches" to your programs such that it checks files before the program loads them or checks E-mail as it comes in).

And, even more insidious are newer E-mail programs that allow one to use programs like Microsoft Word to read and write messages. You may not even know you are using Word. But, since the E-mail program does use Word, macros can be encoded into the message and be made to run on your system when you open the message to read it. It is very important that you know the characteristics of programs you use! Only then will you be able to determine if you are at risk.

Summary

- With macro languages the line between pure data files and executable files is blurring.
- An infected file might be attached to an E-mail. Don't automatically run attached files.
- Be careful of E-mail programs that use other programs with macros to display or create incoming mail.

[Cluster Viruses](#)…

Please visit our sponsors.

Click Here to Visit our Sponsor

What Viruses Infect ||| System Sector | File | Macro | Companion | Cluster | Batch File | Source Code | Visual Basic Worms

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.

[Pray the Rosary](#) for peace.

cknow.com

Virus Types/Methods

Virus Tutorial

Navigation

Virus Types

Tutorial Map

Anti-Virus Software

Companion Viruses

> Companion viruses make use of a DOS quirk that runs COM files before EXE files. The virus infects EXE files by installing a same-named COM file.

Would you believe that a virus can infect your files without changing a single byte in the infected file? Well, it's true; two different ways in fact! The more common of the two ways is called the companion or spawning virus (the other is a cluster virus). The companion virus infects your files by locating all files with names ending in EXE. The virus then creates a matching file name ending in COM that contains the viral code.

Here's what happens: Let's say a companion virus is executing on your PC and decides it's time to infect a file. It looks around and happens to find a file called PGM.EXE. It now creates a file called PGM.COM containing the virus. The virus usually plants this file in the same directory as the .EXE file but it could place it in any directory on your DOS path. If you type PGM and hit enter, DOS will execute PGM.COM instead of PGM.EXE. (In order, DOS will execute COM, then EXE, then BAT files of the same root name, if they are all in the same directory.) The virus executes,

possibly infecting more files and then loads and executes PGM.EXE. The user probably won't notice anything wrong.

This type of virus is fairly easy to detect by the presence of the extra COM files. Sometimes the virus attempts to hide the extra files by either placing them into a different directory (but one on the PATH) or gives them a hidden attribute so a normal DIR command will not show them. And, of course, when the virus is active in memory it can effectively hide the COM files as well (but, unlike many viruses, a companion infector need not remain in memory to do its work).

A good integrity map of what should be on the hard disk can be used to easily detect and clean companion viruses.

Note: There are some instances where it is normal to have both COM and EXE files of the same name (such as DOS 5's DOSSHELL) but this is relatively rare. When this is the case, the companion virus will usually not change the existing COM file (although some are sloppy and will).

Companion viruses were never particularly common and under Windows where specific files are associated with icons you likely won't see them.

Summary

- A companion virus installs a COM file (the virus) for every EXE file found on the disk.
- DOS runs COM files before EXE files and so the virus will run first, going into memory and then will execute the related EXE file.
- Companion viruses are relatively easy to find and eliminate if you have a good integrity map of what should be on your disk.

Batch File Viruses…

Please visit our sponsors.

Click Here to Visit our Sponsor

What Viruses Infect | | | System Sector | File | Macro | Companion | Cluster | Batch File | Source Code | Visual Basic Worms
How Viruses Infect | | | Polymorphic | Stealth | Fast and Slow | Sparse | Armored | Multipartite | Spacefiller | Tunneling |
Camouflage | NTFS ADS | Virus Droppers
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Virus Types/Methods

Virus Tutorial

Navigation

Virus Types

Tutorial Map

Anti-Virus Software

Cluster Viruses

> Cluster viruses change the directory so that when you try to run a program you first run the virus.

There is a type of virus known as a "cluster" virus that infects your files not by changing the file or planting extra files but by changing the DOS directory information so that directory entries point to the virus code instead of the actual program. When you run a program, DOS first loads and executes the virus code, the virus then locates the actual program and executes it. Dir-2 is an example of this type of virus.

The interesting thing about this type of virus is that even though every program on the disk may be "infected," because only the directory pointers are changed there is only one copy of the virus on the disk.

One can also usually classify this type of virus as a fast infector. On any file access, the entire current directory will be infected and, if the DOS path must be searched, all directories on the path will typically be infected.

This type of virus can cause serious problems if you don't

know it's there. While the virus is in memory, it controls access to the directory structure on the disk. If you boot from a clean floppy disk, however, and then run a utility such as SCANDISK the utility will report serious problems with cross-linked files on your disk. Most such utilities will offer to correct the problem and users, not knowing any better, often accept the offer. Unfortunately, in the case of this virus type, if you accept the offer you will end up with all your executable files the same length and each one will be the virus code. **Your original programs will be lost.**

These viruses often use stealth techniques to hide their presence. If you attempt to read the file, the virus will intercept the request and return your original uninfected program to you.

This can sometimes be used to your advantage. If you have a stealth cluster virus (such as Dir-2), you can copy your program files (*.EXE and *.COM files) to files with other extensions and allow the virus to automatically disinfect them! If you "COPY *.COM *.CON" and "COPY *.EXE *.EXX", and then cold boot your PC from a known good copy of DOS on a clean floppy disk and "REN *.CON *.COM" and "REN *.EXX *.EXE", this will effectively disinfect the renamed files.
Note: **This information is presented as an example of a technique that might be used in an emergency when no anti-virus software is available. It's always best to use anti-virus software to clear a virus infection.**

Summary

- A cluster virus changes the directory so the virus is run before any "infected" programs.
- If you boot without the virus in memory a DOS utility will report serious problems, but allowing the utility to fix them will effectively erase any "infected" programs.

Please visit our sponsors.

Click Here to Visit our Sponsor

What Viruses Infect | | | System Sector | File | Macro | Companion | Cluster | Batch File | Source Code | Visual Basic Worms
How Viruses Infect | | | Polymorphic | Stealth | Fast and Slow | Sparse | Armored | Multipartite | Spacefiller | Tunneling |
Camouflage | NTFS ADS | Virus Droppers
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.

Pray the Rosary for peace.

ckNOW.cOm

Virus Types/Methods

Virus Tutorial

Batch File Viruses

Navigation

Virus Types

Tutorial Map

Anti-Virus Software

> Batch files can be used to transmit binary executable code and either be or drop viruses.

While not often found, it is possible to write a batch file that contains a virus. In most cases the batch file is used to drop a memory or disk virus which then takes over when the computer is next started. These don't always work, but it is interesting to briefly go over the design so you can possibly recognize this type of virus if you happen to see one.

One batch file virus takes the following form (it's possible when this page displays you will receive a virus warning if you are running anti-virus software; don't worry, it's just triggering off the partial text below which has the virus code removed):

```
@ECHO OFF
:[ a label of specific form I won't mention ]
COPY %0.BAT C:\Q.COM>NUL
C:\Q
[ binary data ]
```

The first line causes batch file commands to not display on

the screen so you won't see what's going on. The second line is a label as far as the batch file is concerned. In reality, this label is what makes the whole thing work so, of course, we're not going to show any examples. The third line copies the batch file itself to an executable file named Q.COM in the root directory of the C: drive. The output of the COPY command is directed to the NUL device so you see nothing on the screen that indicates this copy took place. Finally, the fourth line executes the newly created Q.COM file.

On the surface you would think that trying to rename a .BAT file to .COM and execute it would result in nothing but errors. Normally, that is the case but the label changes all that. The text up to the label converts to instructions the CPU can execute, but they do nothing. When the label is "executed" this changes. The CPU interprets the label as instructions that cause the CPU to look ahead to the binary instructions in the batch file. These binary instructions are the real virus (or virus dropper).

There are several batch file viruses, but each works in a manner similar to that described above. The labels and batch file instructions may differ; but the method of operation is similar.

Use the characteristics of the virus described above to look for batch file viruses. If there are obscure labels (lines starting with a colon) at the start of a batch file, use caution. Most batch file labels are fairly straightforward words or names. Secondly, if you see a batch file that is several thousand bytes long yet when you use the DOS command TYPE to display it to the screen you only see a few lines, that is another tip-off. Most batch file viruses insert an end-of-file mark (Control-Z) between the batch file portion and the binary instruction portion.

Batch file viruses are not common; but be aware they do exist and have been seen in the wild. Indeed, a new worm version surfaced in early June 2002: Cup. This beast is complicated and arrives attached to an E-mail. If executed,

Cup creates, executes, and sometimes deletes the files WORLDCUP_SCORE.VBS, EYEBALL.REG, JAPAN.VBS, ENGLAND.VBS, IRELAND.VBS, URAGUAY.VBS and ARGENTINA.BAT. The first file mass mails a file called WORLDCUP.BAT to your Outlook address book. The .REG file assures the worm is run at system start by changing the Windows registry. The worm has other payloads in the various .VBS files. So, you see that batch file viruses/worms can be fairly complicated.

Summary

- Batch files can be used to transmit binary executable code and either be or drop viruses.
- To detect these viruses look for two signs:
  - An odd label at the start of the batch file
  - A batch file that is too large for the text in it.

Source Code Viruses…

Please visit our sponsors.

Click Here to Visit our Sponsor

What Viruses Infect ||| System Sector | File | Macro | Companion | Cluster | Batch File | Source Code | Visual Basic Worms
How Viruses Infect ||| Polymorphic | Stealth | Fast and Slow | Sparse | Armored | Multipartite | Spacefiller | Tunneling |
Camouflage | NTFS ADS | Virus Droppers
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

---

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.

CKNOW.COM

Virus Tutorial

Please visit our sponsors.

Source Code Viruses

> **Source code found on your system can be infected; usually by adding Trojan code to it.**

Navigation

Virus Types

Tutorial Map

Anti-Virus Software

While rare, it is possible to infect actual programming source code found on your computer.

Source code comes in many forms because of the many different types of compilers and languages available. This is one reason why source code viruses are not particularly common. The other is that so few people actually write programs it becomes difficult for a source code-only virus to find victims to infect.

Also, because of programming style and differing designs that individuals use when they write program code it's difficult to write a virus that actually spreads via this mechanism. More typically, a source code virus will not infect via source code but simply add Trojan material to existing source code so that when it is compiled and run it does something different than expected.

Die Hard is one example of a type of source code virus. The virus actually spreads by infecting COM and EXE files (a file

virus) but, as part of its payload, in drops Trojan code into any ASM (assembly language) and PAS (Pascal) source files as they are accessed (when the virus is resident in memory).

Source code viruses are not common; but be aware they do exist and have been seen in the wild in the past.

Summary

- Source code viruses add instructions to existing programming code found on your system.
- They are rare and the code they add is typically a Trojan instead of a full virus.

Visual Basic Worms…

What Viruses Infect ||| System Sector | File | Macro | Companion | Cluster | Batch File | Source Code | Visual Basic Worms
How Viruses Infect ||| Polymorphic | Stealth | Fast and Slow | Sparse | Armored | Multipartite | Spacefiller | Tunneling |
Camouflage | NTFS ADS | Virus Droppers
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Pray the Rosary for peace.

cknow.com

Virus Tutorial

Please visit our sponsors.

Click Here to Visit our Sponsor

Navigation

Virus Types

Tutorial Map

Anti-Virus Software

Visual Basic Worms

> **Visual Basic Script files can be used for malicious purposes; particularly in the role of worms.**

The exploit currently the rage seems to be Visual Basic Script (VBS) worms. What is VBS? Let's see what Microsoft says:

> Microsoft® Visual Basic® Scripting Edition, a subset of the Microsoft® Visual Basic® programming language, is a fast, portable, lightweight interpreter for use in World Wide Web browsers and other applications that use Microsoft® ActiveX® Controls, Automation servers, and Java applets.

Basically, think about VBScript as a super batch language. VBScript is an interpreted language (so scripts are really the source code for whatever needs to be done). Scripts can be embedded into such things as web pages or can be standalone files (with the extension .VBS usually).

If you've got Microsoft's Internet Explorer 5 browser on your system it's likely you also have the Windows Scripting Host

(WSH) which is the program used to interpret and run VBS scripts.

Even though VBScript is a scaled down language it is quite capable and can be used to, for example, connect to Microsoft's Outlook mail routines and send files to anyone in your address book. This, of course, makes it possible for VBScript to be a language used by worms to spread themselves.

VBScript can be disabled on your system. We have a page that tells you how to do this if you wish.

Summary

- VBScript is a language that can easily be used to create worms that send themselves and possibly files from your computer to others on the Internet.
- Consider turning scripting off to prevent your accidentally running a malicious script.

How Viruses Infect…

What Viruses Infect ||| System Sector | File | Macro | Companion | Cluster | Batch File | Source Code | Visual Basic Worms
How Viruses Infect ||| Polymorphic | Stealth | Fast and Slow | Sparse | Armored | Multipartite | Spacefiller | Tunneling |
Camouflage | NTFS ADS | Virus Droppers
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Send mail to webmaster@cknow.com with questions or comments about this web site.

[Pray the Rosary](#) for peace.

ccnow.com

Virus Tutorial

How viruses Infect

Navigation

Virus Types

Tutorial Map

Anti-Virus Software

Viruses are sometimes also categorized by how they infect. These categorizations often overlap the categories above and may even be included in the description (e.g., polymorphic file virus). These categories include:

- **Polymorphic Viruses**
  Viruses that change their characteristics as they infect.
- **Stealth Viruses**
  Viruses that try to actively hide themselves from anti-virus or system software.
- **Fast and Slow Infectors**
  Viruses that infect in a particular way to try to avoid specific anti-virus software.
- **Sparse Infectors**
  Viruses that don't infect very often.
- **Armored Viruses**
  Viruses that are programmed to make disassembly difficult.
- **Multipartite Viruses**
  Viruses that may fall into more than one of the top classes.
- **Cavity (Spacefiller) Viruses**
  Viruses that attempt to maintain a constant file size

when infecting.

- **Tunneling Viruses**
  Viruses that try to "tunnel" under anti-virus software while infecting.
- **Camouflage Viruses**
  Viruses that attempted to appear as a benign program to scanners.
- **NTFS ADS Viruses**
  Viruses that ride on the alternate data streams in the NT File System.

Polymorphic Viruses…

What Viruses Infect ||| System Sector | File | Macro | Companion | Cluster | Batch File | Source Code | Visual Basic Worms
How Viruses Infect ||| Polymorphic | Stealth | Fast and Slow | Sparse | Armored | Multipartite | Spacefiller | Tunneling |
Camouflage | NTFS ADS | Virus Droppers
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.

Pray the Rosary for peace.

ccnow.com

Virus Types/Methods

Virus Tutorial

Polymorphic Viruses

Navigation

Virus Types

Tutorial Map

Anti-Virus Software

> **Polymorphic viruses change themselves with each infection. There are even virus-writing toolkits available to help make these viruses.**

To confound virus scanning programs, virus writers created polymorphic viruses. These viruses are more difficult to detect by scanning because each copy of the virus looks different than the other copies. One virus author even created a tool kit called the "Dark Avenger's Mutation Engine" (also known as MTE or DAME) for other virus writers to use. This allows someone who has a normal virus to use the mutation engine with their virus code. If they use the mutation engine, each file infected by their virus will have what appears to be totally different virus code attached to it. Fortunately, the code isn't totally different and now anyone foolish enough to use the mutation engine with their virus will be creating a virus that will be immediately detected by most of the existing scanners.

Virus Tool Kits

Besides the mutation engine, there are also now several tool

kits available to help people create viruses. Several of these programs allow someone who has no knowledge of viruses to create their own "brand new" virus. One of these tool kits even has a very slick user interface with pull down menus and on-line help. You just pick your choices from the various menus and in a flash you've created your very own virus. While this sounds like a pretty ominous development for scanning technology, it's not as bad as it sounds. All the existing tool kits (such as VCS, VCL and MPC) create viruses that can be detected easily with existing scanner technology. The danger with these tool kits lies in the fact it's possible to create such a tool kit that could create viruses that really are unique. Fortunately, this hasn't been done yet, but it's only a matter of time before such a tool kit will be created. The conflict between virus writers and anti-virus researchers continues.

Summary

- Polymorphic viruses change with each infection. They do this in an attempt to defeat scanners.
- Virus writing tool kits have been created to "simplify" creation of new viruses.

Stealth Viruses… Next

What Viruses Infect | | | System Sector | File | Macro | Companion | Cluster | Batch File | Source Code | Visual Basic Worms
How Viruses Infect | | | Polymorphic | Stealth | Fast and Slow | Sparse | Armored | Multipartite | Spacefiller | Tunneling |
Camouflage | NTFS ADS | Virus Droppers
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If

you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Virus Tutorial

Stealth Viruses

Navigation

Virus Types

Tutorial Map

Anti-Virus Software

> **A virus must change things in order to infect a system. In order to avoid detection, a virus will often take over system functions likely to spot it and use them to hide itself. A virus may or may not save the original of things it changes so using anti-virus software to handle viruses is always the safest option.**

A virus, by its nature, has to modify something in order to become active. This might be a file, the boot sector, or partition sector (Master Boot Record); whatever it is, it has to change. Unless the virus takes over portions of the system in order to manage accesses to the changes it made, these changes will become visible and the virus will be exposed.

A stealth virus hides the modifications it makes. It does this by taking over the system functions which read files or system sectors and, when some other program requests information from portions of the disk the virus has changed, the virus reports back the correct (unchanged) information instead of what's really there (the virus). Of course, the virus must be resident in memory and active to do this.

Use of stealth is the major reason why most anti-virus programs operate best when the system is started (booted) from a known-clean floppy disk. When this happens, the virus does not gain control over the system and the changes and virus are immediately available to be seen and dealt with.

Important Note: Some viruses, when they infect, encrypt and hide the original information in the sector they infect. If you are infected, some people may advise you to use generic DOS commands (e.g., SYS and/or FDISK /MBR) to correct the problem. **If you do this you run the risk of making matters much worse.** Monkey, for example, encrypts the partition information and moves it. If you overwrite the virus with FDISK /MBR then you will no longer be able to see your hard disk as DOS/Windows will not recognize what's in the partition table and can't access the encrypted version without Monkey helping (anti-virus software knows how to get around this problem).

Never use undocumented commands (e.g., FDISK /MBR) to fix virus contamination.

Always use an anti-virus package that can deal with the particular virus in question.

Undocumented commands are undocumented for a reason!

Summary

- In order to infect, a virus must change something.
- A stealth virus takes over portions of the system to effectively hide the virus from casual (and not so casual) examination.
- To better find stealth viruses be certain to cold boot from a known-clean (write protected) floppy disk and avoid using generic DOS commands to try to fix them.

Use anti-virus software to handle these viruses.

Fast and Slow Infectors...

Please visit our sponsors.

Click Here to Visit our Sponsor

What Viruses Infect ||| System Sector | File | Macro | Companion | Cluster | Batch File | Source Code | Visual Basic Worms
How Viruses Infect ||| Polymorphic | Stealth | Fast and Slow | Sparse | Armored | Multipartite | Spacefiller | Tunneling |
Camouflage | NTFS ADS | Virus Droppers
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

---

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Virus Tutorial

Please visit our sponsors.

Click Here to Visit our Sponsor

Fast and Slow Infectors

Navigation

Virus Types

Tutorial Map

Anti-Virus Software

A fast infector infects any file accessed, not just run. A slow infector only infects files as they are being created or modified.

The term *fast* or *slow* when dealing with viruses pertains to how often and under what circumstances they spread the infection.

Typically, a virus will load itself into memory when an infected program is run. It sits there and waits for other programs to be run and infects them at that time.

A **fast infector** infects programs not just when they are run, but also when they are simply accessed. The purpose of this type of infection is to ride on the back of anti-virus software to infect files as they are being checked. By its nature, anti-virus software (a scanner, in particular) opens each file on a disk being checked in order to determine if a virus is present. A fast infector that has not been found in memory before the scanning starts will spread itself quickly throughout the disk.

A **slow infector** does just the opposite. A slow infector will

only infect files when they are created or modified. Its purpose is to attempt to defeat integrity checking software by piggybacking on top of the process which legitimately changes a file. Because the user knows the file is being changed, they will be less likely to suspect the changes also represent an infection. By its nature (and because executable code is not usually changed) a slow infector does not spread rapidly and if the integrity checker has a scanning component it will likely be caught. Also, an integrity checker that is run on a computer booted from a known-clean floppy disk will be able to defeat a slow infector.

Summary

- A fast infector infects programs when they are accessed, not just when run. This type of virus is designed to ride on the back of anti-virus scanners and can quickly infect an entire disk if not found before the scan is performed.
- A slow infector infects programs only when they are created or modified. This type of virus is designed to defeat integrity checkers but can usually be found if the checker has a scanner component or is started properly.

[Sparse Infectors](#)…

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

ckmow.com

Virus Tutorial

Please visit our sponsors.

Navigation

Virus Types

[Tutorial Map](#)

[Anti-Virus Software](#)

Sparse Infectors

> **This type of virus uses any one of a variety of techniques to minimize detection of its activity.**

In order to spread widely, a virus must attempt to avoid detection. To minimize the probability of its being discovered a virus could use any number of different techniques. It might, for example, only infect every 20th time a file is executed; it might only infect files whose lengths are within narrowly defined ranges or whose names begin with letters in a certain range of the alphabet. There are many other possibilities.

A virus which uses such techniques is termed a sparse infector.

Summary

- A wide variety of techniques can be used to help a virus avoid detection of its activity.

[Armored Viruses](#)… Next

Please visit our sponsors.

What Viruses Infect | | | System Sector | File | Macro | Companion | Cluster | Batch File | Source Code | Visual Basic Worms
How Viruses Infect | | | Polymorphic | Stealth | Fast and Slow | Sparse | Armored | Multipartite | Spacefiller | Tunneling |
Camouflage | NTFS ADS | Virus Droppers
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Virus Tutorial

Navigation

Virus Types

Tutorial Map

Anti-Virus Software

Armored Viruses

An armored virus attempts to make disassembly difficult.

Armored is a class that overlaps other classes of viruses; maybe multiple times.

Basically, an armored virus uses special "tricks" designed to foil anti-virus researchers. Any anti-virus researcher who wants to find out how a virus works must follow the instruction codes in the virus. By using a variety of methods, virus writers can make this disassembly task quite a bit more difficult. This usually make the virus larger as well.

Such a virus can be said to be armored.

An early virus, Whale, made extensive use of these techniques.

Summary

- An armored virus attempts to make disassembly difficult.

Next

Please visit our sponsors.

Click Here to Visit our Sponsor

What Viruses Infect | | | System Sector | File | Macro | Companion | Cluster | Batch File | Source Code | Visual Basic Worms
How Viruses Infect | | | Polymorphic | Stealth | Fast and Slow | Sparse | Armored | Multipartite | Spacefiller | Tunneling |
Camouflage | NTFS ADS | Virus Droppers
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.

Pray the Rosary for peace.

cknow.com

Virus Types/Methods

Virus Tutorial

Navigation

Virus Types

Tutorial Map

Anti-Virus Software

Multipartite Viruses

> **Multipartite viruses have a dual personality. Some are file viruses that can infect system sectors; others are system sector infectors that can infect files.**

Some viruses can be all things to all machines. Depending on what needs to be infected, they can infect system sectors or they can infect files. These rather universal viruses are termed multipartite (multi-part).

Sometimes the multipartite virus drops a system sector infector; other times a system sector infector might also infect files.

Multipartite viruses are particularly nasty because of the number of ways they can spread. Fortunately, a good one is hard to write.

Summary

- Multipartite viruses have dual capabilities and typically infect both system sectors and files.

Please visit our sponsors.

Click Here to Visit our Sponsor

What Viruses Infect | | | System Sector | File | Macro | Companion | Cluster | Batch File | Source Code | Visual Basic Worms
How Viruses Infect | | | Polymorphic | Stealth | Fast and Slow | Sparse | Armored | Multipartite | Spacefiller | Tunneling |
Camouflage | NTFS ADS | Virus Droppers
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Virus Types/Methods

Virus Tutorial

Cavity (Spacefiller) Viruses

Navigation

Virus Types

Tutorial Map

Anti-Virus Software

> **A cavity (spacefiller) virus attempts to install itself inside of the file it is infecting. This is difficult but has become easier with new file formats designed to make executable files load and run faster.**

Most viruses take the easy way out when infecting files; they simply attach themselves to the end of the file and then change the start of the program so that it first points to the virus and then to the actual program code. Many viruses that do this also implement some stealth techniques so you don't see the increase in file length when the virus is active in memory.

A cavity (spacefiller) virus, on the other hand, attempts to be clever. Some program files, for a variety of reasons, have empty space inside of them. This empty space can be used to house virus code. A cavity virus attempts to install itself in this empty space while not damaging the actual program itself. An advantage of this is that the virus then does not increase the length of the program and can avoid the need for some stealth techniques. The Lehigh virus was an early example of a cavity virus.

Because of the difficulty of writing this type of virus and the limited number of possible hosts, cavity viruses are rare…however… A new Windows file format known as Portable Executable (PE) is designed to make loading and running programs faster. While a great goal, the implementation has the effect of leaving potentially large gaps in the program file. A cavity (spacefiller) virus can find these gaps and insert itself into them. The CIH virus family takes advantage of this new file format. There will likely be more. (For more info about PE files see the Computer Knowledge PE Info Page.)

Summary

- A cavity virus attempts to install itself inside of the file it is infecting.
- In the past this was difficult to do properly, but new file formats make it easier.

Tunneling Viruses…

What Viruses Infect | | | System Sector | File | Macro | Companion | Cluster | Batch File | Source Code | Visual Basic Worms
How Viruses Infect | | | Polymorphic | Stealth | Fast and Slow | Sparse | Armored | Multipartite | Spacefiller | Tunneling |
Camouflage | NTFS ADS | Virus Droppers
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Send mail to webmaster@cknow.com with questions or comments about this web site.

Pray the Rosary for peace.

cknow.com

Virus Tutorial

Navigation

Virus Types

Tutorial Map

Anti-Virus Software

Tunneling Viruses

> Some viruses will attempt to tunnel under anti-virus monitoring programs in order to bypass their monitoring functions.

One method of virus detection is an interception program which sits in the background looking for specific actions that might signify the presence of a virus. To do this it must intercept interrupts and monitor what's going on. A tunneling virus attempts to backtrack down the interrupt chain in order to get directly to the DOS and BIOS interrupt handlers. The virus then installs itself underneath everything, including the interception program. Some anti-virus programs will attempt to detect this and then reinstall themselves under the virus. This might cause an interrupt war between the anti-virus program and the virus and result in problems on your system.

Some anti-virus programs also use tunneling techniques to bypass any viruses that might be active in memory when they load.

Summary

- A tunneling virus attempts to bypass activity monitor anti-virus programs by following the interrupt chain back down to the basic DOS or BIOS interrupt handlers and then installing itself.

Camouflage Viruses…

What Viruses Infect | | | System Sector | File | Macro | Companion | Cluster | Batch File | Source Code | Visual Basic Worms
How Viruses Infect | | | Polymorphic | Stealth | Fast and Slow | Sparse | Armored | Multipartite | Spacefiller | Tunneling |
Camouflage | NTFS ADS | Virus Droppers
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Virus Types/Methods

Virus Tutorial

Navigation

Virus Types

Tutorial Map

Anti-Virus Software

Camouflage Viruses

> When scanners were less sophisticated it might have been possible for a virus to sneak by as scanners sometimes did not display some alarms, knowing them to be false. This type of virus would be extremely hard to write today.

You don't hear much about this type of virus. Fortunately it is rare and, because of the way anti-virus programs have evolved, is unlikely to occur in the future.

When anti-virus scanners were based completely on signatures there was always the possibility of a false alarm when the signature was found in some uninfected file (a statistical possibility). Further, with several scanners circulating, each had their own signature database and when scanned by another product may indicate infection where there was none simply because of the inclusion of the virus identification string. If this happened often, the public would get understandably annoyed (and frightened). In response, a scanner might therefore implement logic that, under the right circumstances, would ignore a virus signature and not issue an alarm.

While this "skip it" logic would stop the false alarms, it opened a door for virus writers to attempt to camouflage their viruses so that they included the specific characteristics the anti-virus programs were checking for and thus have the anti-virus program ignore that particular virus. Fortunately, this never became a serious threat; but the possibility existed.

Today's scanners do much more than simply look for a virus signature string. In order to identify the specific virus variant they also check the virus code and even checksum the virus code to identify it. With these cross-checks it would be extremely difficult for a virus to camouflage itself and spoof a scanner.

Summary

- In the past it was possible for a virus to spoof a scanner by camouflaging itself to look like something the scanner was programmed to ignore.
- Because of scanner technology evolution this type of virus would be very difficult to write today.

NTFS ADS Viruses…

What Viruses Infect | | | System Sector | File | Macro | Companion | Cluster | Batch File | Source Code | Visual Basic Worms
How Viruses Infect | | | Polymorphic | Stealth | Fast and Slow | Sparse | Armored | Multipartite | Spacefiller | Tunneling |
Camouflage | NTFS ADS | Virus Droppers
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small

payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
[Pray the Rosary](#) for peace.

ckmow.com

Virus Types/Methods

Virus Tutorial

Navigation

Virus Types

Tutorial Map

Anti-Virus Software

NTFS ADS Viruses

The NT File System allows alternate data streams to exist attached to files but invisible to some file-handling utilities. A virus can exploit such a system.

The NT File System (NTFS) contains within it a system called Alternate Data Streams (ADS). This subsystem allows additional data to be linked to a file. The additional data, however, is not always apparent to the user. Windows Explorer and the DIRectory command do not show you the ADS; other file tools (e.g., COPY and MOVE) will recognize and process the attached ADS file.

The basic notation of an ADS file is <filename>:<ADSname>. A simple example that creates an ADS file is probably the best way to illustrate this. At the system prompt use the ECHO command to create a file and then you can also use ECHO to create an ADS attachment to that file **(if doing this, create a directory/folder specifically for the test)**.

ECHO "This is the test file" > testfile.txt

You should now have a file called TESTFILE.TXT in your test directory. The TYPE, EDIT, and NOTEPAD commands should be able to access this file and show you its contents and a directory command will show it to be about 23 bytes long. The TESTFILE.TXT file was created in what's called the "named stream" portion of the file system. Now create an alternate data stream file:

> ECHO "This is text in the ADS file" > testfile.txt:teststream1.txt

Note that this new file is in the format described above: <filename>:<ADSname>.

But, now try to find this new file. A directory command does not show it; the TYPE and EDIT commands won't find it. The command…

> NOTEPAD testfile.txt:teststream1.txt

…will bring it into the editing area; but even NOTEPAD will only read the file; you can't do a File|SaveAs and try to create an ADS file with NOTEPAD. Most other programs will not see the ADS file at all. You should also note that you've added about 30 bytes to the original file but a directory command on testfile.txt only shows the original size. **The ADS file is effectively hidden from view.**

Further, an alternate stream file can be created that has no normal stream file association. Here is why it's suggested you try these experiments in a test directory. Try:

> ECHO "This is a really invisible stream file." > :invisible.txt

This file will be created but will be completely invisible to any directory commands or Windows Explorer.

Finally, you may have some trouble trying to delete the stream files you just created. The DEL command does not

work with ADS files so DEL :invisible.txt, for example, does not work. The main way to delete alternate stream files associated with a normal stream file is to delete the normal stream file. All ADS files associated with that file will also be deleted. So DEL testfile.txt would have to be used for the first test file created. The :invisible.txt file will be deleted when the directory the file is in is removed.

If you need to keep the main file but delete the stream(s) attached to it there are two ways to proceed:

- Copy the file to a FAT or FAT32 partition and then back again to the NTFS partition. This effectively strips the ADS files off of the primary file.
- Use the NT Resource Kit CAT utility. You'll have to rename the file, use CAT on it, and then delete the temporary file you created. The syntax would be:

> REN needtokeep.exe temp.exe
> CAT temp.exe > needtokeep.exe
> DEL temp.exe

Virus Use

An alternate stream file can be an executable and executed in a variety of ways. For our purposes here the files can be exploited by viruses that make their way into files saved as part of the normal stream. In one such exploit the virus (Streams) creates a copy of itself as a temporary EXE file and then copies the original EXE file as an ADS file attached to the temporary EXE file. The temporary EXE file is then renamed to the original EXE name. Now, when the user tries to run the original file they actually run the virus which does its thing and then sends the original program file to the operating system which then runs the program. The only thing you might see is a slight delay in program start.

For a virus like Streams you should not just delete an infected file. If you do the original file will also be lost as

it's attached. If your anti-virus software does not provide a recovery utility you will have to use the CAT utility in a manner similar to that described above:

> CAT filename.exe:STR newname.exe *(this copies the original file to "newname.exe")*
>
> COPY /B newname.exe filename.exe *(this copies "newname.exe" back to its original name and overwrites the virus)*

The virus can be operating system specific. Streams, for example, checks for Windows 2000 and only runs if it's found.

There are other ways a virus might use an alternate data stream. It could, for example, hide most of its code attached to files not normally scanned by virus scanners (e.g., INI or other text files). Only a small executable that extracts the virus would have to be visible and might be easier to hide. There are more malicious things a virus could do as well (please don't ask).

Summary

- The NT File System allows alternate data streams to exist attached to files but invisible to some normal file-handling utilities.
- Viruses can exploit the NTFS ADS system in a variety of ways.

Virus Droppers…

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Virus Types/Methods

Virus Tutorial

Virus Droppers

A dropper is a program that, when run will attempt to install a regular virus onto your hard disk.

Navigation

Virus Types

Tutorial Map

Anti-Virus Software

Normally, you obtain a virus by either attempting to boot from an infected floppy disk, by running an infected file, or by loading an infected document with viral macro commands in it. There is another way you can pick up a virus: by encountering a virus dropper. These are rare, but now and again someone will attempt to be clever and try to program one.

Basically, a dropper is just what the name implies: a program designed to run and install (or "drop") a virus onto your system. The program itself is not infected nor is it a virus because it does not replicate. So, technically, a dropper should be considered a Trojan. Often, because the virus is hidden in the program code, a scanner will not detect the danger until after the virus is dropped onto your system. (It's technically possible to write a virus that also drops other viruses, and several have been tried. Most are very buggy, however.)

It's a technical point, but there is a class of dropper that

only infects the computer's memory, not the disk. These are given the name injector by some virus researchers.

Summary

- A Trojan program that installs a virus onto your system is called a dropper.
- Fortunately, because of technical difficulties, droppers are hard to program and therefore rare.

That's it for the discussion of virus types. Before going on to protection let's take an interesting detour…

[Virus History](#)…

Please visit our sponsors.

Click Here to Visit our Sponsor

What Viruses Infect ||| System Sector | File | Macro | Companion | Cluster | Batch File | Source Code | Visual Basic Worms
How Viruses Infect ||| Polymorphic | Stealth | Fast and Slow | Sparse | Armored | Multipartite | Spacefiller | Tunneling |
Camouflage | NTFS ADS | Virus Droppers
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Dr. Solomon History

Virus Tutorial

Narrative histories are available from several sources. The information in this section was provided by and used with permission of Dr. Solomon Software. Dr. Solomon's is now a part of Network Associates....

A Brief History of PC Viruses

by
Dr. Alan Solomon

Navigation

History Detail

Tutorial Map

Anti-Virus Software

Next

Please visit our sponsors.

Click Here to Visit our Sponsor

Dr. Solomon's History ||| 1986-1987 | 1988 | 1989 | 1990 | 1991 | 1992 | 1993 | The Future
Robert Slade's History ||| Earliest Virus History | Early Related | Fred Cohen | Pranks/Trojans | Apple Virus | Lehigh/Jerusalem |
(c) Brain | MacMag
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Dr. Solomon History

Virus Tutorial

Navigation

Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats

History Detail

Tutorial Map

Anti-Virus Software

1986-1987 - The Prologue

It all started in 1986. Basit and Amjad realised that the boot sector of a floppy diskette contained executable code, and this code is run whenever you start up the computer with a diskette in drive A. They realised that they could replace this code with their own program, that this could be a memory resident program, and that it could install a copy of itself on each floppy diskette that is accessed in any drive. The program copied itself; they called it a virus. But it only infected 360KB floppy disks.

In 1987, the University of Delaware realised that they had this virus, when they started seeing the label "(c) Brain" on floppy diskettes. That's all it did; copy itself, and put a volume label on diskettes.

Meanwhile, also in 1986, a programmer called Ralf Burger realised that a file could be made to copy itself, by attaching a copy of itself to other files. He wrote a demonstration of this effect, which he called VIRDEM. He distributed it at the Chaos Computer Club conference that December, where the theme was viruses. VIRDEM would infect any COM file; again the payload was pretty harmless.

This attracted so much interest, that he was asked to write a book. Ralf hadn't thought of boot sector viruses like Brain,

so his book doesn't even mention them. But by then, someone had started spreading a virus, in Vienna.

In 1987, Franz Swoboda became aware that a virus was being spread in a program called Charlie. He called it the Charlie virus. He made lots of noise about the virus (and got badly bitten as a result). At this point, there are two versions of the story, Burger claims that he got a copy of this virus from Swoboda, but Swoboda denies this. In any case, Burger obtained a copy, and gave it to Berdt Fix, who disassembled it (this was the first time anyone had disassembled a virus). Burger included the disassembly in his book, after patching out a couple of areas to make it less infectious and changing the payload. The normal payload of Vienna is to cause one file in eight to reboot the computer (the virus patches the first five bytes of the code); Burger (or maybe Fix) replaced this reboot code with five spaces. The effect was that patched files hung the computer, instead of rebooting. This isn't really an improvement.

Meanwhile, in the US, Fred Cohen had completed his doctoral dissertation, which was on computer viruses. Dr Cohen proved that you cannot write a program that can, with 100% certainty, look at a file and decide whether it is a virus. Of course, no one ever thought that you could, but Cohen made good use of an existing mathematical theorem and earned a doctorate. He also did some experiments; he released a virus on a system, and discovered that it travelled further and faster than anyone had expected.

In 1987, Cohen was at Lehigh, as was Ken van Wyk. So was the author of the Lehigh virus. Lehigh was an extremely unsuccessful virus - it never managed to spread outside its home university, because it could only infect COMMAND.COM and did a lot of damage to its host after only four replications. One of the rules of the virus is that a virus that quickly damages it host, cannot survive. However, the Lehigh virus got a lot of publicity, and led to van Wyk setting up the Virus-L newsgroup on Usenet. Lehigh was nasty. After four replications, it did an overwrite on the

disk, hitting most of the File Allocation Table. But a virus that only infects COMMAND.COM, isn't very infectious.

Meanwhile, in Tel Aviv, Israel (some say in Italy), another programmer was experimenting. His first virus was called Suriv-01 (virus spelled backwards). It was a memory resident virus, but it could infect any COM file, whereas Lehigh could only infect COMMAND.COM. This is a much better infection strategy than the non-TSR strategy used by Vienna, as it leads to files on all drives and all directories being infected. His second virus was called Suriv-02, and that could infect only EXE files, but it was the first EXE infector in the world. His third attempt was called Suriv-03, and it could handle COM and EXE files. His fourth effort escaped into the world, and became known as the Jerusalem virus. Every Friday 13th, instead of infecting files that are run, it deletes them. But Friday 13ths are not common, so the virus is pretty inconspicuous, most of the time. It avoids infecting COMMAND.COM, because in those days, many people believed that this was the file to watch (see Lehigh).

It looks as if it escaped rather than was released, because it plainly was not ready for release. The author decided to change the way that the virus detected itself in EXE files, and had made part of that change. There is redundant code from the Suriv viruses still in place, and also what looks like debugging code. It was found in the Hebrew University of Jerusalem (hence the name) by Yisrael Radai.

While all this was going on, a young student at the University of Wellington, New Zealand, had found a very simple way to create a very effective virus. One time in eight, when booting from an infected floppy, it also displayed the message 'Your PC is now Stoned', hence the name of the virus.

The virus itself was just a few hundred bytes long, but because of its self-restraint, and memory-resident replication, it has become the most widespread virus in the world, accounting for over a quarter of outbreaks. It is very

unlikely that Stoned virus will ever become rare. The virus spread rapidly, because of its inconspicuousness (and because in those days, people were keeping a careful eye on COMMAND.COM, because of Lehigh).

In Italy, at the University of Turin, a programmer was writing another boot sector virus. This one put a bouncing ball up on the screen, if the disk was accessed exactly on the half hour. It became known as Italian virus, Ping Pong, or Bouncing Ball. But this virus had a major defect; it couldn't work on anything except an 8088 or 8086 computer, because it uses an instruction that doesn't work on more advanced chips. As a result, this virus has almost died out (as has Brain, which can only infect 360KB floppies, and which foolishly announces its presence via the volume label).

Back in the US, an American was demonstrating a problem that has continued to dog US virus writers ever since: incompetence. The Lehigh didn't make it outside a small circle; neither did the Yale virus. This was another boot sector virus, but it only copied itself when you booted from an infected floppy, then put another floppy in to continue the boot process. No subsequent diskette was infected, and if the boot-up continued from a hard disk, there was no infection at all. Yale never spread at all widely, either.

But also in 1987, a German programmer was writing a very competent virus, the Cascade, so called after the falling letters display that it gave. Cascade used a new idea - most of the virus was encrypted, leaving only a small stub of code in clear for decrypting the rest of the virus. The reason for this was not clear, but it certainly made it more difficult to repair infected files, and it restricted the choice of search string to the first couple of dozen bytes. This idea was later extended by Mark Washburn when he wrote the first polymorphic virus, 1260 (Chameleon). Washburn based Chameleon on a virus that he found in a book: the Vienna, published by Burger.

Cascade was supposed to look at the BIOS, and if it found an IBM copyright, it would refrain from infecting. This part of the code didn't work. The author soon released another version of the virus, 1704 bytes long instead of 1701, in order to correct this bug. But the corrected version had a bug that meant that it still didn't detect IBM BIOSes.

Of these early viruses, only Stoned, Cascade and Jerusalem are common today, but those three are very common.

[Onward to 1988](#)…

Dr. Solomon's History ||| 1986-1987 | 1988 | 1989 | 1990 | 1991 | 1992 | 1993 | The Future
Robert Slade's History ||| Earliest Virus History | Early Related | Fred Cohen | Pranks/Trojans | Apple Virus | Lehigh/Jerusalem |
(c) Brain | MacMag
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

---

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

cknow.com

Dr. Solomon History

Virus Tutorial

1988 - The Game Begins

Navigation

History Detail

Tutorial Map

Anti-Virus Software

The year 1988 was fairly quiet, as far as virus writing went. Mostly, it was the year that anti-virus vendors started appearing, making a fuss about what was at that time only a potential problem, and not selling very much anti-virus software. The vendors were all small companies, selling their software for very low prices (#5 or $10 was common). Some of them were shareware, some were freeware. Occasionally some larger company tried to pop up, but no-one was paying serious cash to solve a potential problem.

In some ways, that was a pity, because 1988 was a very virus-friendly year. It gave Stoned, Cascade and Jerusalem a chance to spread undetected, and to establish a pool of infected objects that will ensure that they never become rare.

It was in 1988 that IBM realised that it had to take viruses seriously. This was not because of the well-known Christmas tree worm, which was pretty easy to deal with. It was because IBM had an outbreak of Cascade at the Lehulpe site, and found itself in the embarrassing position of having to inform its customers that they might have become infected there. In fact, there was no real problem, but from this point on, IBM took viruses very seriously indeed, and the High Integrity Computing Laboratory in Yorktown was given

responsibility for the IBM research effort in this field.

1988 saw a few scattered, sporadic outbreaks of Brain, Italian, Stoned, Cascade and Jerusalem. It also saw the final arguments about whether viruses existed or not. Peter Norton, in an interview, said that they were an urban legend, like the crocodiles in the New York sewers, and one UK expert claimed that he had a proof that viruses were a figment of the imagination. In 1988, the real virus experts would debate with such people; after that year, real virus experts would simply walk away from anyone who had such absurd beliefs.

Each outbreak of a virus was dealt with on a case-by-case basis. One American claimed that he had a fully equipped mobile home for dealing with virus outbreaks (and another one extrapolated to the notion that soon there would be many such mobile units). Existing software was used to detect boot sector viruses (by inspecting the boot sector), and one-off software was written for dealing with outbreaks of Cascade and Jerusalem.

In 1988, a virus that is called "Virus-B" was written. This is another virus that doesn't go memory resident, and it is a modification of another virus that deletes files on Friday 13th. When this virus is run, it displays "WARNING!!!! THIS PROGRAM IS INFECTED WITH VIRUS-B! IT WILL INFECT EVERY .COM FILE IN THE CURRENT SUBDIRECTORY!". A virus that is as obvious as that, was clearly not written to spread. It was obviously written as a demonstration virus. Virus researchers are often asked for "harmless viruses" or "viruses for demonstration"; most researchers offer some alternative, such as an overhead foil, or a non-virus program that does a falling letters display. But it looks as if VIRUS-B was written with the intention of giving it away as a demonstration virus - hence the warning. And, indeed, we find that an American company was offering it to "large corporations, universities and research organizations" on a special access basis.

At the end of 1988, a few things happened almost at once.

The first was a big outbreak of Jerusalem at a large financial institution, which meant that dozens of people were tied up in doing a big clean-up for several days. The second was that a company called S&S did the first ever Virus Seminar that actually explained what a virus was and how they worked. The third was Friday 13th. [S&S became what was known as Dr. Solomon Software, which has subsequently been purchased by Network Associates.]

It was clear that we couldn't go out and help everyone with a virus, even if we bought a mobile home and equipped it (with what)? It was also clear that the financial institution, and the academic site, could easily handle a virus outbreak, but they didn't have the tools to do the job. All they needed was a decent virus detector, which was not available. So we wrote one, added some other tools that experience said might be useful, and created the first Anti-Virus Toolkit.

In 1989, the first Friday 13th was in January. At the end of 1988, it was clear that Jerusalem was in Spain and the UK, at least, and was in academic as well as commercial sites. Because of the destructive payload in the virus, we felt that if we failed to send out some sort of warning, we would be negligent. But the media grabbed the ball and ran with it; the predictability of the trigger day, together with the feature of it being Friday 13th, caught their imagination, and the first virus media circus was under way.

On the 13th of January, we had dozens of phone calls, mostly from the media wanting to know if the world had ended yet. But we also had calls from a large corporate site, a small vendor of PC hardware, and a couple of single users. We were invaded by TV cameras in droves, and had to schedule them carefully to avoid them tripping over each other. In the middle of all this, the PC Support person from the infected corporation arrived. The TV people wanted nothing better than a victim to film, but the corporate person wanted anonymity. We pretended that he was just one of our staff. Also, at that time, British Rail contacted us; they also had an outbreak of Jerusalem, and they went

public on it. Later, they regretted that decision, because for a long time afterwards, their PC Support person was badgered by the media seeking interviews.

Onward to 1989…

Please visit our sponsors.

Click Here to Visit our Sponsor

Dr. Solomon's History | | | 1986-1987 | 1988 | 1989 | 1990 | 1991 | 1992 | 1993 | The Future
Robert Slade's History | | | Earliest Virus History | Early Related | Fred Cohen | Pranks/Trojans | Apple Virus | Lehigh/Jerusalem |
(c) Brain | MacMag
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.

Pray the Rosary for peace.

cknow.com

Dr. Solomon History

Virus Tutorial

Navigation

History Detail

Tutorial Map

Anti-Virus Software

1989 - Datacrime

During 1989 things really started to move. The Fu Manchu virus (a modification of Jerusalem) was sent anonymously to a virus researcher in the UK, and the 405 virus (a modification of the overwriting virus in the Burger book) was sent to another UK researcher. A third UK researcher wrote a virus and sent it to another UK researcher; in 1989, the UK was where it was all happening. But not quite all. In 1989, the Bulgarians started getting interested in viruses, and Russia was beginning to awaken.

In March of 1989, a minor event happened that was to trigger an avalanche. A new virus was written in Holland. A Dutchman calling himself Fred Vogel (a very common Dutch name) contacted a UK virus researcher, and said that he had found this virus all over his hard disk. He also said that it was called Datacrime, and that he was worried that it would trigger on the 13th of the next month.

When the virus was disassembled, it was found that on any day after October 12th, it would trigger a low level format of cylinder zero of the hard disk, which would, on most hard disks, wipe out the File Allocation Table, and leave the user effectively without any data. It would also display the virus' name: Datacrime virus. A straightforward write-up of the effect of this virus was published, but it was another non-

memory-resident virus, and so highly unlikely to spread.

However, the write-up was reprinted by a magazine, another magazine repeated the story, a third party embellished it a bit, and by June it was becoming an established fact that it would trigger on October 12th (not true, it triggers on any day *after* the 12th, up till December 31st) and that it would low level format the whole hard disk. In America, the press started calling it "Columbus Day virus" (October 12th) and it was suggested that it had been written by Norwegian terrorists, angry at the fact that Eric the Red had discovered America, not Columbus.

Meanwhile, in Holland, the Dutch police were doing one of the things that falls within those things that police are supposed to do: crime prevention. Datacrime virus was obviously a crime, and the way to prevent it was to run a detector for it. So they commissioned a programmer to write a Datacrime detector, and offered it at Dutch police stations for $1. It sold really well. But it gave a number of false alarms, and it had to be recalled and replaced with version 2. There were long queues outside the Dutch police stations, lots of confusion about whether anyone actually had this virus (hardly anyone did, but the false alarms muddied the waters).

If the police take something seriously, it must be serious, right? So in July, large Dutch companies started asking IBM if viruses were a serious threat. Datacrime isn't, but there is a distinct possibility that a company could get Jerusalem, Cascade or Stoned (or Italian, in those days before 8088 computers became a rarity). So what is IBM doing about this threat, they asked?

IBM had internal-use-only anti-virus software. They used this to check incoming media, and to make sure that an accident like Lehulpe could never happen again. IBM had a problem: if they didn't offer this software to their customers, they could look very bad if on October 13th a lot of computers went down. The technical people knew that this wouldn't

happen, but obviously they knew that someone, somewhere, might have important data on a computer that would get hit by Datacrime. IBM had to make a decision about whether to release their software, and they had a very strict deadline to work to; October the 13th would be too late.

In September of 1989, IBM sent out version 1.0 of the IBM scanning software, together with a letter telling their customers what it was, and why they were sending it out. When you get a letter like that from IBM, and a disk, you would be pretty brave to take no notice, so a lot of large companies scanned a lot of computers, for the first time. Hardly anyone found Datacrime, but there were instances of the usual viruses.

October 13th fell on a Friday, so there was a double event: Jerusalem and Datacrime. In the US, Datacrime (Columbus Day) had been hyped out of all proportion for a virus that is as uninfective as this one, and it is highly likely that not a single user had the virus. In Europe (especially in Holland) there might have been a few, but not many.

In London, the Royal National Institute for the Blind announced that they'd had a hit, and had lost large amounts of valuable research data, and months of work. We investigated this particular incident, and the truth was that they had a very minor outbreak of Jerusalem, and a few easily-replaced program files had been deleted. Four computers were infected. But the RNIB outbreak has passed into legend as a Great Disaster. Actually, the RNIB took more damage from the invasion of the television and print media than from the virus.

By the end of 1989, there were a couple of dozen viruses that we knew about, but we didn't know that in Bulgaria and Russia, big things were brewing.

Please visit our sponsors.

Click Here to Visit our Sponsor

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Dr. Solomon History

Virus Tutorial

Navigation

History Detail

Tutorial Map

Anti-Virus Software

1990 - The Game Gets More Complex

By 1990, it was no longer a matter of running a couple of dozen search strings down each file. Mark Washburn had taken the Vienna virus, and created the first polymorphic virus from it. We didn't use that word at first, but the idea of his viruses (1260, V2P1, V2P2 and V2P6) was that the whole virus would be variably encrypted, and there would be a decryptor at the start of the virus. But the decryptor could take a very wide number of forms, and in the first few viruses, the longest possible search string was just two bytes long (V2P6 got this down to one byte). To detect this virus, it was necessary to write an algorithm that would apply logical tests to the file, and decide whether the bytes it was looking at were one of the possible decryptors.

One consequence of this, was that some vendors couldn't do this. It isn't easy to write such an algorithm, and many vendors were, by this time, relying on search strings extracted by someone else. The three main sources of search strings were a newsletter called Virus Bulletin, the IBM scanner, and reverse engineering a competitor's product. But you can't detect a polymorphic virus this way (indeed, two years after these viruses were published, many products are [were] still incapable of detecting these

viruses). Washburn also published his source code, which is now widely available. At the time, we thought that this would bring out a number of imitators; in practice, no-one seems to be using Washburn's code. However, plenty of virus authors are using his idea.

Another consequence of polymorphic viruses, was an increase in the false alarm rate. If you write code to detect something that has as many possibilities as V2P6, then there is a chance that you will flag an innocent file, and that chance is much greater than with the sort of virus that you can find with a 24-byte scan string. A false alarm can be as much hassle to the user as a real virus, as he will put all his anti-virus procedures into action.

Also, in 1990, we saw a number of virus coming out of Bulgaria, especially from someone who called himself "Dark Avenger." The Dark Avenger viruses introduced two new ideas. The first idea was the "Fast infector"; with these viruses, if the virus is in memory, then simply opening a file for reading, triggers the virus infection. The entire hard disk is very soon infected. The second idea in this virus, was that of subtle damage. Dark Avenger-1800 occasionally overwrites a sector on the hard disk. If this isn't noticed for a period of time, the corrupted files are backed up, and when the backup is restored, the data is still no good. Dark Avenger targets backups, not just data. Other viruses came from the same source, such as the Number-of-the-Beast (stealth in a file virus) and Nomenklatura (with an even nastier payload than Dark Avenger).

Also, Dark Avenger was more creative about distributing his viruses. He would upload them to BBSes, infecting shareware anti-virus programs, together with a documentation file that gave reassurance to anyone who checked the file size and checksums. He uploaded his source code also, so that people could learn how to write viruses.

In 1990, another event happened in Bulgaria - the first virus exchange BBS. The idea was that if you uploaded a virus,

you could download a virus, and if you uploaded a new virus, you were given full access. This, of course, encourages the creation of new viruses, and gets viruses into wider circulation. Also, the VX BBS offered source code, which makes the technology of writing a virus more widely available.

In the second half of 1990, the Whale appeared. Whale was a very large, and very complex virus. It didn't do very much; mostly, it crashed the computer when you tried to run it. But it was an exercise in complexity and obfuscation, and it arrived in virus author's hands like a crossword puzzle to be solved. Some virus researchers wasted weeks unraveling Whale, although in practice you could detect it with a couple of dozen search strings, and you didn't really need to do any more, as the thing was too clumsy to work anyway. But because it was so large and complex, it achieved fame.

At the end of 1990, the anti-virus people saw that they had to get more organised; they had to be at least as organised as the virus authors. So EICAR (European Institute for Computer Antivirus Research) was born in Hamburg, in December 1990. This gave a very useful forum for the anti-virus researchers and vendors to meet and exchange ideas (and specimens), and to encourage the authorities to try to prosecute virus authors more vigorously. At the time that EICAR was founded, there were about 150 viruses, and the Bulgarian "Virus factory" was in full swing.

Onward to 1991…

Dr. Solomon's History | | | 1986-1987 | 1988 | 1989 | 1990 | 1991 | 1992 | 1993 | The Future
Robert Slade's History | | | Earliest Virus History | Early Related | Fred Cohen | Pranks/Trojans | Apple Virus | Lehigh/Jerusalem |
(c) Brain | MacMag

file:///C|/Documents%20and%20Settings/Owner/My...WeaverWebs/ComputerKnowledge/vtutor/vt1990.htm (3 of 4) [6/19/2002 11:45:15 AM]

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
[Pray the Rosary](#) for peace.

ckmow.com

Dr. Solomon HIstory

Virus Tutorial

1991 - Product Launches and Polymorphism

Navigation

History

Detail

Tutorial Map

Anti-Virus Software

In 1991, the virus problem was sufficiently interesting to attract the large marketing companies. Symantec launched Norton Anti-Virus in December 1990, and Central Point launched CPAV in April 1991. This was soon followed by Xtree, Fifth Generation and a couple of others. Most of these companies were rebadging other company's programs (nearly all Israeli). The other big problem of 1991 was "glut." In December 1990, there were about 200-300 viruses; by December 1991 there were 1,000 (there may have been even more written that year, because by February, we were counting 1,300).

Glut means lots of viruses, and this causes a number of unpleasant problems. In every program, there must be various limitations. In particular, a scanner has to store search strings in memory, and under DOS, there is only 640KB to use (and DOS, the network shell and the program's user interface might take half of that).

Another Glut problem, is that some scanners slow down in proportion to the number of viruses scanned for. Not many scanners work this way, but it certainly poses a problem for those that do.

A third Glut problem, comes with the analysis of viruses; this is necessary if you want to detect the virus reliably, to repair it, and if you want to know what it does. If it takes one researcher one day to disassemble one virus, then he can only do 250 per year. If it takes one hour, that figure becomes 2,000 per year, but whatever the figure, more viruses means more work.

Glut also means a lot of viruses that are similar to each other. This then can lead to mis-identification, and therefore a wrong repair. Very few scanners attempt a complete virus identification, so this confusion about exactly which virus is being found, is very common.

Most of these viruses came from Eastern Europe and Russia; the Russian virus production was in full swing. But another major source of new viruses was the virus exchange BBSes.

Bulgaria pioneered the VX BBS, but a number of other countries quickly followed. Some shut down not long after they started up, but the Milan "Italian Virus Research Laboratory" was where a virus author called Cracker Jack uploaded his viruses (which were plagiarised versions of the Bulgarian viruses). Germany had Gonorrhea, Sweden had Demoralised Youth, America had Hellpit, UK had Dead On Arrival and Semaj. Some of these have now either closed down or gone underground, but they certainly contributed to the glut problem. With a VX BBS, all a virus author has to do, is download some source code, make a few simple changes, then upload a new virus, which gives him access to all the other viruses on the board.

1991 was also the year that polymorphic viruses first made a major impact on users. Washburn had written 1260 and the V2 series long before, but because these were based on Vienna, they weren't infectious enough to spread. But in April of 1991, Tequila burst upon the world like a comet. It was written in Switzerland, and was not intended to spread. But it was stolen from the author by a friend, who planted it on his father's master disks. Father was a

shareware vendor, and soon Tequila was very widespread.

Tequila used full stealth when it installed itself on the partition sector, and in files it used partial stealth, and was fully polymorphic. A full polymorphic virus is one for which no search string can be written down, even if you allow the use of wild cards. Tequila was the first polymorphic virus that was widespread. By May, the first few scanners were detecting it, but it was not until September that all the major scanners could detect it reliably. If you don't detect it reliably, then you miss, say, 1% of infected files. The virus starts another outbreak from these overlooked instances, and has to be put down again, but now there is that old 1%, plus another 1% of files that are infected but not detected. This can continue for as long as the user has patience, until eventually the hard disk contains nothing but files that the scanner cannot detect. The user, thinks that after the virus coming back a number of times, it gradually infected fewer and fewer files, until now he has gotten rid of it completely.

In September 1991, Maltese Amoeba spread through Europe - another polymorphic virus. By the end of the year, there were a few dozen polymorphic viruses. Each of these is classified as "difficult," meaning it takes a virus researcher more than a few hours to do everything that needs to be done. Also, most products need some form of hard coding in order to detect the virus, which means program development, which means bugs, debugging, beta testing and quality control. Furthermore, although a normal virus won't slow down most scanners, a polymorphic virus might.

It was also in 1991, that Dark Avenger announced the first virus vapourware. He threatened a virus that had 4,000,000,000 different forms. In January 1992, this virus appeared, but it wasn't a virus.

[Onward to 1992](...)…

Send mail to webmaster@cknow.com with questions or comments about this web site.
Pray the Rosary for peace.

cknow.com

Dr. Solomon History

Virus Tutorial

Please visit our sponsors.

Click Here to Visit our Sponsor

Navigation

History

Detail

Tutorial Map

Anti-Virus Software

1992 - Michelangelo

January 1992 saw the Self Mutating Engine (MtE) from Dark Avenger. At first, all we saw was a virus that we named Dedicated, but shortly after that, we saw the MtE. This came as an OBJ file, plus the source code for a simple virus, and instructions on how to link the OBJ file to a virus to give you a full polymorphic virus. Immediately, virus researchers set to work on detectors for it. Most companies did this in two stages. In some outfits, stage one was look at it and shudder, stage two was ignore it and hope it goes away. But at the better R&D sites, stage one was usually a detector that found between 90 and 99% of instances, and was shipped very quickly, and stage two was a detector that found 100%. At first, it was expected that there would be lots and lots of viruses using the MtE, because it was fairly easy to use this to make your virus hard to find. But the virus authors quickly realised that a scanner that detected one MtE virus, would detect all MtE viruses fairly easily. So very few virus authors have taken advantage of the engine (there are about a dozen or two viruses that use it).

This was followed by Dark Avenger's Commander Bomber. Before CB, you could very easily predict where in the file the virus would be. Many products take advantage of this predictability to run fast; some only scan the top and tail of

the file, and some just scan the one place in the file that the virus must occupy if it is there at all. Bomber transforms this, and so products either have to scan the entire file, or else they have to be more sophisticated about locating the virus.

Another virus that came out at about that time, was Starship. Starship is a fully polymorphic virus (to defeat scanners), with a few neat anti-debugging tricks, and it also aims to defeat checksummers with a very simple trick. Checksumming programs aim to detect a virus by the fact that it has to change executable code in order to replicate. Starship only infects files as they are copied from the hard disk to the floppy. So files on the hard disk never change. But the copy on the floppy disk is infected, and if you then copy that onto a new hard disk, and tell the checksummer on the new machine about this new file, the checksummer will happily accept it, and never report any changes. Starship also installs itself on the hard disk, but without changing executable code. It changes the partition data, making a new partition as the boot partition. No code is changed, but the new partition contains the virus code, and this is run before it passes control on to the original boot partition.

Probably the greatest event of 1992 was the great Michelangelo scare. One of the American anti-virus vendors forecast that five million computers would go down on March the 6th, and many other US vendors climbed on to the bandwagon. PC users went into a purchasing frenzy, as the media whipped up the hype. On March the 6th, between 5,000 and 10,000 machines went down, and naturally the US vendors that had been hyping the problem put this down to their timely and accurate warning. We'll probably never know how many people had Michelangelo, but certainly in the days leading up to March the 6th, a lot of computers were checked for viruses. After March 6th, there were a lot of discredited experts around.

The reaction to the Michelangelo hype did a lot of damage

to the credibility of people advocating sensible antivirus strategies, and outweighed any possible benefits from the gains in awareness.

In August 1992, we saw the first serious virus authoring packages. First the VCL (Virus Creation Laboratory) from Nowhere Man, and then Dark Angel's Phalcon/Skism Mass-Produced Code Generator. These packages made it possible for anyone who could use a computer, to write a virus. Within twelve months, dozens of viruses had been created using these tools.

Towards the end of 1992, a new virus writing group called ARCV (Association of Really Cruel Viruses) had appeared in England - within a couple of months, the Computer Crime Unit of New Scotland Yard had tracked them down and arrested them. ARCV flourished for about three months, during which they wrote a few dozen viruses and attracted a few members.

Another happening of 1992, was the appearance of people selling (or trying to sell) virus collections. To be more precise, these were collections of files, some of which were viruses, and many of which were assorted harmless files. In America, John Buchanan offered his collection of a few thousand files for $100 per copy, and in Europe, The Virus Clinic offered various options from #25. The Virus Clinic was raided by the Computer Crime Unit; John Buchanan is [?| still offering viruses for sale.

Towards the end of 1992, the US Government was offering viruses to people who called the relevant BBS.

Onward to 1993…

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

ckhow.com

Virus Tutorial

Navigation

History Detail

Tutorial Map

Anti-Virus Software

1993 - Polymorphics and Engines

Early in 1993, XTREE announced that they were quitting the antivirus business. This was the first time that a major company had given up the struggle.

Early in 1993, a new virus writing group appeared, in Holland, called Trident. The main Trident author, Masouf Khafir, wrote a polymorphic engine called the Trident Polymorphic Engine, and released a virus that used it, called GIRAFE. This was followed by updated versions of the TPE. The TPE is much more difficult to detect reliably than the MtE, and very difficult to avoid false alarming on.

Khafir also released the first virus that worked according to a principle first described by Fred Cohen. The Cruncher virus was a data compression virus, that automatically added itself to files in order to auto-install on as many computers as possible.

Meanwhile, Nowhere Man, of the Nuke group, had been busy. Early in 1993, he released the Nuke Encryption Device (NED). This was another mutator that was more tricky than MtE. A virus called Itshard soon followed.

Phalcon/Skism was not to be left out. Dark Angel released DAME (Dark Angel's Multiple Encyptor) in an issue of 40hex; a virus called Trigger uses this. Trident released version 1.4 of TPE (again, this is more complex and difficult than previous versions) and released a virus called Bosnia that uses it.

Soon after that, Lucifer Messiah, of Anarkick Systems had taken version 1.4 of the TPE and written a virus POETCODE, using a modified version of this engine (1.4b).

Early in 1993, another highly polymorphic virus appeared, called Tremor. This rocketed to stardom when it got included in a TV broadcast of software (received via a decoder).

In the middle of 1993, Trident got a boost when Dark Ray and John Tardy joined the group. Tardy released a fully polymorphic virus in 444 bytes, and we can expect more difficult things from Trident.

The main events of 1993, were the emergence of an increasing number of polymorphic engines, which will make it easier and easier to write viruses that scanners find difficult to detect.

Onward to the future…

Dr. Solomon's History ||| 1986-1987 | 1988 | 1989 | 1990 | 1991 | 1992 | 1993 | The Future
Robert Slade's History ||| Earliest Virus History | Early Related | Fred Cohen | Pranks/Trojans | Apple Virus | Lehigh/Jerusalem |
(c) Brain | MacMag
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you

will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Virus Tutorial

Please visit our sponsors.

Click Here to Visit our Sponsor

Navigation

History Details

Tutorial Map

Anti-Virus Software

The Future

There will be more viruses - that's an easy prediction. How many more is a difficult call, but over the last five years, the number of viruses has been doubling every year or so. This surely must slow down. If we say 1,500 viruses in mid-1992, and 3,000 in mid-1993, then we could imagine 5,000 in mid 1994 and we could expect to reach the 8,000 mark some time in 1995. Or perhaps we are being optimistic? [The number topped 10,000 in 1996. It continues to go up.]

The glut problem will continue, and could get sharply worse. Whenever a group of serious anti-virus researchers meet, we find an empty room, hang "Closed for cleaning" on the door, and frighten each other with "nightmare scenarios." Some of the older nightmare scenarios have already come true, others have not, but remain possibilities. The biggest nightmare for all anti-virus people is glut. There are only about 10-15 first class anti-virus people in the world, and most of the anti-virus companies have just one of these people (some have none). It would be difficult to create more, as the learning curve is very steep. The first time you disassemble something like Jerusalem virus, it takes a week. After you've done a few hundred viruses, you could whip through something as simple as Jerusalem in 15 minutes.

The polymorphic viruses will get more numerous. It turns out that they are a much bigger problem than the stealth viruses, because stealth is aimed at checksummers, but polymorphism is aimed at scanners, which is what most people are using. And each polymorphic virus will be a source of false alarms, and will cause the researchers much more work than the normal viruses.

The polymorphic viruses will also continue to get more complex, as virus authors learn the technique, and increasingly try to ensure that their viruses cannot be detected.

Scanners will get larger - more code will be needed because more viruses will need hard coding to scan for them. The databases that scanners use will get larger; each new virus needs to be detected, identified and repaired. Loading the databases will take longer, and some programs will have memory shortage problems. [Indeed, this has forced anti-virus firms to combine more sophisticated techniques with simple database scanning.]

As Windows becomes more popular, people will be increasingly reluctant to run scanners under DOS. But if you are running Windows, you have run software on the hard disk, and if one of the things you've run is infected by a virus, you have a virus in memory. If there is a virus in memory, you cannot trust what the computer is saying - it could be a stealth virus. Windows will make antivirus software less secure.

The R&D effort to keep scanners up-to-date will get more and more. Some companies won't be able to do it, and will decide that scanning is outdated technology, and try to rely on checksumming. Other companies will licence scanners from one of the few companies that still maintains adequate R&D (we've already started seeing some of this). Some companies will decide that the anti-virus business isn't as profitable as they had thought, and will abandon their anti-

virus product, and go back to their core business.

Users will get a lot more relaxed about viruses. We've long since passed the stage where a virus is regarded as a loathsome disease, to be kept secret. But we're increasingly seeing people who regard a virus on their system with about the same degree of casualness as a bit of fluff on their jacket. Sure, they'll wipe it off, but there's not real need to worry about it happening again. This is perhaps a bit too relaxed an attitude, but what can you expect if a user keeps on getting hit by viruses, and nothing terrible ever seems to result.

Anti-virus products will mature a lot. Those without any kind of decent user interface will have a hard time competing against the pretty ones. Those with a long run time will be rejected in favour of those that run in seconds. Exactly which viruses are detected will have far less emphasis (it is very difficult for users to swallow claims about so many thousands of viruses) than the ease of use of the product, and the amount of impact it has on the usability of the computer.

New products will keep arriving, as each company invents the product that makes all previous products obsolete. Sometimes the magic ingredient will be software (AI, neural nets, whatever is the latest buzzword) and sometimes it will be hardware (which can never be infected, except that that isn't the problem). These products will burst on a startled world in a blaze of publicity, and vanish without trace when users find that installing them makes their computer unusable, or else it doesn't find any viruses, or both. But new ones will come along to take their place.

Gradually, people will trade up from DOS to whatever takes its place; OS/2, Windows-NT or Unix, and the DOS virus will become as irrelevant as CP/M. Except that DOS will still be around 10 or even 20 years from now, and viruses for the new operating system will start to appear as soon as it is worth writing them.

Some computers are already being built with ingrained resistance to viruses. Some brands of computer are already immune to boot sector viruses, provided you make a simple choice in the CMOS setup (don't boot from the floppy). ["Immune" is probably too strong as a multipartite virus can still drop a boot sector infector from a file even if the CMOS is set to only boot from the hard disk.] Right now, very few users are being told that these computers can be set up that way, but people are gradually finding out for themselves. This doesn't solve the virus problem, but anything that makes the world a difficult place for viruses must be a help.

The virus problem will be with us forever. It isn't the dramatic, worldshaking kind of problem that Michelangelo was made out to be; nor is it the fluff-on-your-jacket kind of problem. But as long as people have problems with computers, other people will be offering solutions for those problems.

Thank you Dr. Solomon.

[Go on to Robert M. Slade's History](...)…

Dr. Solomon's History ||| 1986-1987 | 1988 | 1989 | 1990 | 1991 | 1992 | 1993 | The Future
Robert Slade's History ||| Earliest Virus History | Early Related | Fred Cohen | Pranks/Trojans | Apple Virus | Lehigh/Jerusalem |
(c) Brain | MacMag
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Send mail to webmaster@cknow.com with questions or comments about this web site.

Pray the Rosary for peace.

cknow.com

Robert Slade History

Virus Tutorial

Narrative histories are available from several sources. Robert M. Slade's is a somewhat more technically oriented history and is available here with permission…

History of Computer Viruses

by
Robert M. Slade

Navigation

History Detail

Tutorial Map

Anti-Virus Software

Robert Slade has also written or contributed to books about viruses. His latest is shown here…

[Viruses Revealed](#)

by
David Harley, Urs E. Gattiker, Robert Slade

Paperback-400 pages (August 2001) Osborne McGraw-Hill
(I'm told Computer Knowledge is mentioned in Chapter 8!)

Next

Click Here to Visit our Sponsor

Dr. Solomon's History | | | 1986-1987 | 1988 | 1989 | 1990 | 1991 | 1992 | 1993 | The Future
Robert Slade's History | | | Earliest Virus History | Early Related | Fred Cohen | Pranks/Trojans | Apple Virus | Lehigh/Jerusalem |
(c) Brain | MacMag
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
[Pray the Rosary](#) for peace.

ckncow.com

Virus Tutorial

Navigation

History Detail

Tutorial Map

Anti-Virus Software

Earliest History of Viral Programs

Viral programs have a long, and sometimes honourable, history. (I do not intend, by this statement, to be involved in the current debate about whether or not viral programs serve a useful purpose outside research environments.)

In the earliest computers it was vital that you knew the initial state of the computer. It was also important that no remnants of other programs remain. (It is hard enough to debug programs now: you don't need extraneous "noise" to deal with.) An instruction was often implemented that had only one function: it would copy itself to the next memory location and then proceed on to that location. Thus, by starting this instruction at the beginning of memory, the entire memory space could be "filled" with a known value. This single instruction could be seen as the first viral type program.

As computers progressed, it became possible to run more than one program at a time in a single machine. It was, of course, important that each program, and its associated data, be contained within certain bounds, or partitions. Inevitably, there were programs which "broke the bounds", and would either perform operations on the data or

programs belonging to different procedures, or actually transferred control to random areas and tried to execute data as program instructions. Random operations and damage would result. Attempts to trace the "path" of damage or operation would show "random" patterns of memory locations. Plotting these on a printout map of the memory looks very much like the design of holes in "worm-eaten" wood: irregular curving traces which begin and end suddenly. The model became known as a "wormhole" pattern, and the rogue programs became known as "worms". In an early network of computers a similar program, the infamous "Xerox worm", not only broke the bounds within its own computer, but spread from one computer to another. This has led to the use of the term "worm" to differentiate a viral program that spreads over networks from other types. The term is sometimes also used for viral programs which spread by some method other than attachment to, or association with, program files.

(Programmers being who they are, the development of such rogue programs became a sport. This is now enshrined in the game of "Core Wars". A program is run which "simulates" a computer environment. A standard set of instructions, known as "Redstone code", is used to build programs which battle each other within the simulated environment. The objective is survival. The use of such tactics as attack, avoidance and replication is of interest to virus research, as is the trade-off between complexity of design and chance of destruction.)

[A look at early viral-related programs](#)…

Please visit our sponsors.

Dr. Solomon's History ||| 1986-1987 | 1988 | 1989 | 1990 | 1991 | 1992 | 1993 | The Future

Robert Slade's History ||| Earliest Virus History | Early Related | Fred Cohen | Pranks/Trojans | Apple Virus | Lehigh/Jerusalem |

file:///C|/Documents%20and%20Settings/Owner/My%...rWebs/ComputerKnowledge/vtutor/vtsladeearly.htm (2 of 3) [6/19/2002 11:45:46 AM]

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Robert Slade History

Virus Tutorial

Navigation

History Detail

Tutorial Map

Anti-Virus Software

Early viral related programs

One of the factors involved in the success of viral programs is a study of the mindset of the user: a study of the psychology or sociology of the computer community. Since the spread of viral programs generally require some action, albeit unknowing, on the part of the operator, it is instructive to look at the security breaking aspects of other historical programs.

"Password trojans" are extremely popular in the university and college environments (where most of the new security breaking ideas and pranks tend to come from anyway). These programs can be extremely simple. An easy "painting" of the screen with a facsimile of the normal login screen will generally get the user to enter their name and password. It is quite simple to have a program write this information to a file, or even mail it to a specific account. Most of these programs will then send back a message to the user that the login has been denied; most users will accept this as an indication that they have either a mistake in entering the login data or that there is some unknown fault in the system. Few question it even after repeated refusals. Some programs are sophisticated enough to pass the login information on to another spawned process: few users even know enough to check the level of nesting of processes.

(A famous, if relatively harmless, prank in earlier computers was the "cookie" program which ran on PDP series computers. This program would halt the operation that the victim was working on and present a message requesting a cookie. There are consistent reports of viral programs following this pattern, including a very detailed report of a "Spanish Cookie" virus, however the author has never seen any such program. In the absence of such data I have, regretfully, come to the conclusion that this is another piece of computer folklore which has mutated into legend.)

Another, lesser known, prank has a closer relationship to current viral programs. In the RISKS-FORUM Digest (6-42) in March of 1988 there was a detailed outline of the use of the "intelligent" features of Wyse 75 terminals. This was a specific instance of a general case of the use of intelligent peripherals for security cracking. In this case, the terminal had a feature which would allow keys to be remapped from the host system. Another feature allowed the keys to be called for from the host. This allowed email messages (actually only the subject line) to be composed which would remap a key to correspond to the "kill process and logout" command, and then have the command submitted by the terminal. With only a little thought, an email virus could be written taking advantage of this fact.

[Fred Cohen's contributions](...)… Next

Dr. Solomon's History ||| 1986-1987 | 1988 | 1989 | 1990 | 1991 | 1992 | 1993 | The Future
Robert Slade's History ||| Earliest Virus History | Early Related | Fred Cohen | Pranks/Trojans | Apple Virus | Lehigh/Jerusalem |
(c) Brain | MacMag
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.

Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Robert Slade History

Virus Tutorial

Navigation

History Detail

Tutorial Map

Anti-Virus Software

Fred Cohen

No historical overview of viral programs can be complete without mention of the work of Fred Cohen.

Hi Fred. (Just kidding.)

In the early 1980s, Fred Cohen did extensive theoretical research, as well as setting up and performing numerous practical experiments, regarding viral type programs. His dissertation was presented in 1986 as part of the requirements for a doctorate in electrical engineering from the University of Southern California. This work is foundational, and any serious student of viral programs disregards it at his own risk.

(Dr. Cohen's writings are available for purchase from: ASP Press, PO Box 81270, Pittsburgh, PA 15217, USA.)

Dr. Cohen's definition of a computer virus as "a program that can 'infect' other programs by modifying them to include a … version of itself" is generally accepted as a standard. On occasion it presents problems with the acceptance of, say, boot sector viral programs and entities such as the Internet/UNIX/Morris worm. However, his work did experimentally demonstrate and theoretically prove many vital issues.

I cannot, in one column, describe the sum total of his work. In my opinion, the most important aspects are the demonstration of the universality of risk, and the limitations of protection. His practical work proved the technical feasibility of a viral attack in any computer system environment. (This feat was achieved within a closed environment and could not, by its nature, have predicted the social and psychological factors which have contributed to the pandemic spread of viral programs "in the wild".) Equally important, his theoretical study proved that the "universal" detection of a virus is undecidable. Although monitoring and analytical programs have a place in the antiviral pantheon, this fact means that they, and, in fact, all other antiviral software, can never give 100% guaranteed protection. Without this early work, it is likely that some toilers in the antiviral vineyards would still be pursuing that elusive grail.

Pranks and Trojans…

Please visit our sponsors.

Click Here to Visit our Sponsor

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.

[Pray the Rosary](#) for peace.

cknow.com

Robert Slade History

Virus Tutorial

Navigation

History Detail

Tutorial Map

Anti-Virus Software

Pranks and Trojans

Pranks are very much a part of the computer culture. So much so, that one can now buy commercially produced joke packages which allow you to perform "Stupid Mac (or PC) Tricks". There are numberless pranks available as shareware. Some make the computer appear to insult the user, some use sound effects or voices, some use special visual effects. A fairly common thread running through most pranks is that the computer is, in some way, non-functional. Many pretend to have detected some kind of fault in the computer (and some pretend to rectify such faults, of course making things worse). One recent entry in our own field is PARASCAN, the paranoid scanner. It tends to find large numbers of very strange viral programs, none of which, oddly, have ever appeared in the CARO index. Aside from temporary aberrations of heart rate and blood pressure, pranks do no damage.

I would not say the same of trojans. I distinguish between a prank and a trojan on the basis of intent to damage. The Trojan Horse was the gift with betrayal inside; so a trojan horse program is an apparently valuable package with a hidden, and negative, agenda.

Trojans are sometimes also referred to (less so now than in the past) as "arf arf" programs. One of the first was

distributed as a program the would enable graphics on early TTL monitors. (That **should** have been a giveaway: such an operation was impossible.) When run, it presented a message saying "Gotcha. Arf, arf." while the hard drive was being erased.

Trojan programs are spread almost entirely via public access electronic bulletin boards. Obviously, a damaging program which can be identified is unlikely to be distributed through a medium in which the donor can be identified. There are, as well, BBSes which are definitely hangouts for software pirates, and act as distribution points for security breaking tips and utilities. These two factors have led to a confusion of trojan programs, viral programs and "system crackers" which has proven extremely resistant to correction. It has also led to a view of BBSes as distribution points for viral programs. (Recently our local "tabloid" paper's computer columnist, normally better versed than this, dismissed the availability of antiviral software to combat Michelangelo by saying that no self respecting company would ever use a BBS.) This in spite of the fact that the most successful viral programs, boot sector infectors, cannot be transmitted over BBS systems, at least not without sophisticated intervention (generally at both ends of the transfer.)

The "AIDS" Trojan (not virus)

I'll conclude the introductory history with the AIDS Information Disk trojan for two reasons: 1) it deserves a place in the history of "malware" in any case and 2) it was so widely; and incorrectly; reported as a virus.

In the fall of 1989, approximately 10,000 copies of an "AIDS Information" package were sent out from a company calling itself PC Cyborg. Some were received at medical establishments, a number were received at other types of businesses. The packages appeared to have been professionally produced. Accompanying letters usually referred to them as sample or review copies. However, the packages also contained a very interesting "license

agreement":

> "In case of breach of license, PC Cyborg
> Corporation reserves the right to use program
> mechanisms to ensure termination of the use of
> these programs. These program mechanisms will
> adversely affect other program applications on
> microcomputers. You are hereby advised of the
> most serious consequences of your failure to
> abide by the terms of this license agreement."

Further in the license is the sentence: "Warning: Do not use
these programs unless you are prepared to pay for them".

The disks contained an installation program and a very
simplistic AIDS information "page turner" and risk
assessment. The installation program appeared only to copy
the AIDS program onto the target hard disk, but in reality
did much more. A hidden directory was created with a
nonprinting character name and a hidden program file with
a nonprinting character in the name was installed. The
AUTOEXEC.BAT file was renamed and replaced with one
which called the hidden program, and then the original
AUTOEXEC. The hidden program kept track of the number of
times the computer was rebooted, and, after a certain
number, encrypted the hard disk. The user was then
presented with an invoice and a demand to pay the license
fee in return for the encryption key. Two major "versions"
were found to have been shipped. One, which waited for 90
reboots was thought to be the "real" attempt: an earlier
version which encrypted after one reboot alerted authorities
and was thought to be an error on the part of the principals
of PC Cyborg.

The Panamanian address for PC Cyborg, thought by some to
be a fake, turned out to be a real company. Four principals
were identified, as well as an American accomplish who
seems to have had plans to have sent 200,000 copies to
American firms if the European "test" worked. The trial of
the American has just been suspended, as his bizarre

behaviour in court is seen as an indication of "diminished responsibility".

A little-known Apple II virus… Next

Dr. Solomon's History ||| 1986-1987 | 1988 | 1989 | 1990 | 1991 | 1992 | 1993 | The Future
Robert Slade's History ||| Earliest Virus History | Early Related | Fred Cohen | Pranks/Trojans | Apple Virus | Lehigh/Jerusalem |
(c) Brain | MacMag
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.

Pray the Rosary for peace.

cknow.com

Robert Slade History

Virus Tutorial

Navigation

History Detail

Tutorial Map

Anti-Virus Software

Apple Virus

The earliest case of a virus that succeeded "in the wild" goes back to late 1981, even before the work of Fred Cohen. In fairness, this does not appear to have been noted by many until long after the fact. For the benefit of those who do not delight in flame wars the author will not be identified: those who have followed the history of viri [viruses] will know whom I refer to as Joe :-).

The idea was sparked by a speculation regarding "evolution" and "natural selection" in pirated copies of games at Texas A&M: the "reproduction" of preferred games and "extinction" of poor ones. This led to considerations of programs which reproduced on their own. (I see no reason to doubt the author's contention that there was no malice involved: this was, after all, the first case that we know of. Indeed, it was Joe's contention that a virus had to be relatively "benign" in order to survive.)

Apple II computer diskettes of that time, when formatted in the normal way, always contained the disk operating system. Joe attempted to find the minimum change that would make a version of the DOS that was viral, and then tried to find an "optimal" viral DOS. A group came up with version 1 of such a virus in early 1982, but quarantined it because of adverse effects. Version 2 seemed to have no

negative impact, and was allowed to "spread" through the disks of group members.

Eventually security was relaxed too far and the virus escaped to the general Apple user population. It was only then that the negative impact of the virus was seen: the additional code length caused some programs, and one computer game in particular, to abort. A third version was written which made strenuous efforts to avoid the memory problems: parts of the coding involve bytes which are both data and opcode. Version 3 was subsequently found to have spread into disk populations previously felt to be uninfected, but no adverse reactions were ever reported.

(For those who have Apple DOS 3.3 disks, location B6E8 in memory, towards the end of track 0, sector 0 on disk, should be followed by eighteen zero bytes. If, instead, the text "(GEN xxxxxxx TAMU)" appears, the digits represented by the "x"s should be a generation counter for virus version 3.)

The story has an interesting postscript. In 1984, a malicious virus was found to be spreading through the schools where all this took place. Some disks appeared to have some immunity. These immune disks turned out to all be infected with version 3.

[Lehigh and Jerusalem description](#)... Next

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Robert Slade History

Virus Tutorial

Navigation

History Detail

Tutorial Map

Anti-Virus Software

Lehigh and Jerusalem

The autumn of 1987 really seemed to get the ball rolling with regard to virus research. The first message to awaken interest was sent by one "LUKEN" of Lehigh University. For all the damage that the Lehigh virus caused, we should at least be grateful that it brought us our Peerless Leader (aka krvw).

Not all students are mini-hackers: not all students are even semi computer literate. Student consultants at universities and colleges are presented with a steady stream of disks from which files have "mysteriously" disappeared. In November of 1987, however, it appeared that certain of the failed disks were due to something other than user carelessness.

The Lehigh virus overwrote the stack space at the end of the COMMAND.COM file. (Early reports stated there was no increase in file size: later research showed an increase of 555 bytes in the size of infected files.) When an infected COMMAND.COM was run (usually upon booting from an "infected disk"), the virus stayed resident in memory. When any access was made to another disk, via the TYPE, COPY, DIR or other normal DOS commands, any (and only) uninfected COMMAND.COM files would be infected. A counter was kept of infections: after four infections the

virus would overwrite the boot and FAT areas of disks with contents from the BIOS.

The primary defence of the virus was that, at the time, no one would have been looking for it. The date of infected COMMAND.COM files was altered by the virus, and, when attempting an infection on a write protected disk, the virus would not trap the "WRITE PROTECT ERROR" message (a dead giveaway if all you were doing was a DIR).

The virus was limited in its "target population" to those disks which had a COMMAND.COM file, and, more particularly, those which contained a full operating system. Admittedly, in those heady bygone days, more users kept copies of the operating system on their disks. However, the virus was also self-limiting in that it would destroy itself once activated, and would activate after only four "reproductions". To the best of our knowledge, the Lehigh virus never did spread off the campus in that initial attack. (It is, however, found in a number of private virus collections, and may be "released" into the wild from time to time. As noted, it has little chance of spreading today.)

The "Jerusalem" virus

In the MS-DOS world the Stoned virus is currently the most successful virus in terms of the number of infections (copies or reproductions) that the virus has produced. (Boot sector viral programs seem to have an advantage among microcomputer users.) Among file infecting viral programs, however, the Jerusalem virus is the clear winner. It has another claim to fame as well. It almost certainly has the largest number of variants of any virus program known to date.

Initially known as the "Israeli" virus, the version reported by Y. Radai in early 1988 (also sometimes referred to as "1813" or Jerusalem-B) tends to be seen as the "central" virus in the family. Although it was the first to be very widely disseminated, and was the first to be "discovered" and

publicized, internal examination suggests that it was, itself, the outcome of previous viral experiments. Although one of the oldest viral programs, the Jerusalem family still defies description, primarily because the number of variants makes it very difficult to say anything about the virus for sure. The "Jerusalem" that you have may not be the same as the "Jerusalem" of your neighbour.

A few things are common to pretty much all of the Jerusalem family. They are file, or program, infecting viri [viruses], generally adding themselves to both COM and EXE files. When an infected file is executed, the virus "goes resident" in memory, so that it remains active even after the original infected program is terminated. Programs run after the program is resident in memory are infected by addition of the virus code to the end of the file, with a redirecting jump added to the beginning of the program. Most of the family carry some kind of "date" logic bomb payload, often triggered on Friday the 13th. Sometimes the logic bomb is simply a message, often it deletes programs as they are invoked.

David Chess has noted that it is a minor wonder the program has spread as far as it has, given the number of bugs it contains. Although it tends to work well with COM files, the differing structure of EXE files has presented Jerusalem with a number of problems. The "original Jerusalem", not content with one infection, will "reinfect" EXE files again and again so that they continually grow in size. (This tends to nullify the advantage that the programmer built in when he ensured that the file creation date was "conserved" and unchanged in an infected file.) Also, EXE programs which use internal loaders or overlay files tend to be infected "in the wrong place", and have portions of the original program overwritten.

The history of the Jerusalem virus is every bit as convoluted as its functionality and family. The naming alone is a fairly bizarre tale. As mentioned before, it was originally called the Israeli virus. Although considered unfair by some, it was

fairly natural as the virus had both been discovered and reported from Israel. (Although the virus was reported to slow down systems that were infected, it seems to have been the "continual growth" of EXE files which led to the detection of the virus.) In an effort to avoid anti-semitism, it was referred to by its "infective length" of 1813 bytes. For COM files. For EXE files it was 1808 bytes. Sometimes. It varies because of the requirement that the header of an EXE file is divisible by 16. (All quite clear?)

One of the early infections was found to be in an office belonging to the Israeli Defence Forces. This fact was reported in an Associated Press article, and, of course, made much of. It also gave rise to another alias, the I.D.F. virus.

When the virus was first discovered, it was strongly felt that it had been circulating prior to November of 1987. The "payload" of file deletion on Friday the 13th gave rise to conjecture as to why the logic bomb had not "gone off" on Friday, November 13th, 1987. (Subsequent analysis has shown that the virus will activate the payload only if the year is not 1987.) The next following "Friday the 13th" was May 13th, 1988. Since the last day that Palestine existed as a nation was May 13th, 1948 it was felt that this might have been an act of political terrorism. This led to another alias, the PLO virus. (The fact that Israel celebrates its holidays according to the Jewish calendar, and that the independence celebrations were slated for three weeks before May 13th in 1988 were disregarded. The internal structure of the virus, and the existence of the sURIV viral programs seems to indicate that any political correspondence is merely coincidence.)

Yet another alias is "sUMsDos", based upon text found in the virus code itself. This was, on occasion, corrupted to "sumDOS".

The name "Jerusalem" has gained ascendancy, possibly due to the McAfee SCAN program identification. (He certainly

must be responsible for the "B" designation for the "original" version.) Of course, the great number of variants have not helped any. Because a number of the variants are very closely based upon each others code, the signatures for one variant will often match another, thus generating even more naming confusion. This confusion is not unique to the Jerusalem family, of course, and is an ongoing concern in the virus research community.

Although it is difficult to be absolutely certain about pronouncements as to the provenance and family history of viral programs, it is almost certain that the Jerusalem virus is, in fact, two viral programs combined. Among the Jerusalem "family" are three "sURIV" variants (again, named for text in the code.) It is fairly easy to see where "virus" 1, 2 and 3 come from. sURIV 1.01 is a COM file infector, COM being the easier file structure and therefore the easier programs to infect. sURIV 2 is an EXE only infector, and is considerably longer and more complex code. sURIV 3 infects both types of program files, and has considerable duplication of code: it is, in fact, simply the first two versions "stuck" together.

(Although the code in the sURIV programs and the "1813" version of Jerusalem is not absolutely identical, all the same features are present. The date of the "payload" is April 1 in the sURIV variants. There is also a "year" condition: some of the payload of the sURIV variants is not supposed to "go off" until after 1988.)

Perhaps this explains the "popularity" of the Jerusalem virus as a "template" for variants. The code is reasonably straightforward and, for those with some familiarity with assembly programming, an excellent "primer" for the writing of viral programs affecting both COM and EXE files. (There is, of course, the fact that Jerusalem is both "early" and "successful". There are many copies of Jerusalem "in the wild", and it may be simply availability that has made it so widely copied. Its "value" as a teaching tool may simply be an unfortunate coincidence.)

Of course, not every virus writer who used the Jerusalem as a template showed the same good taste and imagination in what they did with it. Not all of them even fixed the obvious flaws in the original. The "variations" tend to be quite simplistic: there are a number of "Thursday the 12th", "Saturday the 14th" and "Sunday the 15th" programs. (Some of the "copy cat" virus authors added errors of their own. One of the "Sunday" variants is supposed to delete files on the "seventh" day of the week. Unfortunately, or perhaps fortunately for those of us in the user community, nobody ever bothered to tell the author that computers start counting from zero and Sunday is actually the "zeroth" day of the week. The file deletions never actually happen.)

[The (c) Brain virus](#)...

Please visit our sponsors.

Click Here to Visit our Sponsor

Dr. Solomon's History | | | 1986-1987 | 1988 | 1989 | 1990 | 1991 | 1992 | 1993 | The Future
Robert Slade's History | | | Earliest Virus History | Early Related | Fred Cohen | Pranks/Trojans | Apple Virus | Lehigh/Jerusalem |
(c) Brain | MacMag
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

ccnow.com

Robert Slade History

Virus Tutorial

Please visit our sponsors.

Navigation

History Detail

Tutorial Map

Anti-Virus Software

(c) Brain

The "Brain" virus is probably the earliest MS-DOS virus. At one time it was the most widespread of PC viral programs. (Yet more support for the "superiority" of boot sector viral programs in terms of numbers of infections.) Extensive study has been done on the Brain family, and those wishing further details should consult Alan Solomon's analyses (which, unfortunately, are too detailed for full inclusion in the Anti-Virus Toolkit). In spite of this, and in spite of the existence of address and phone number information for the supposed author, we still have no first, second or even third hand reports of the production of the virus, and so little can be said with absolute certainty. (We do have a first hand report from the author of the Den Zuk variant, for which I am grateful to Fridrik Skulason.)

The Brain "family" is prolific, although less so than Jerusalem. (Seemingly, any "successful" virus spawns a plague of copies as virus-writer-wannabes use it as a template.) Again, like the Jerusalem, it seems that one of the lesser variants might be the "original". The "ashar" version appears to be somewhat less sophisticated than the most common "Brain", and Brain contains text which makes no sense unless it is "derived" from ashar. Brain contains other "timing" information: a "copyright" date of 1986, and an apparent "version" number of 9.0.

Brain is a boot sector infector, somewhat longer than some of the more recent BSIs. Brain occupies three sectors itself, and, as is usual with BSIs, repositions the normal boot sector in order to "mimic" the boot process. As the boot sector is only a single sector, Brain, in infecting a disk, reserves two additional sectors on the disk for the remainder of itself, plus a third for the original boot sector. This is done by occupying unused space on the diskette, and then marking those sectors as "bad" so that they will not be used and overwritten. The "original" Brain virus is relatively harmless. It does not infect hard disks, or disks with formats other than 360K. (Other variants are less careful, and can overlay FAT and data areas.)

Brain is at once sly and brazen about its work. It is, in fact, the first "stealth" virus, in that a request to view the boot sector of an infected disk, on an infected system will result in a display of the original boot sector. However, the Brain virus is designed **not** to hide its light under a bushel in another way: the volume label of infected diskettes becomes "(c) Brain" (or "(c) ashar" or "Y.C.1.E.R.P" for different variants). Hence the name of the virus.

Who wrote the Brain virus?

Well, it's quite simple really. In one of the most common Brain versions you will find text, unencrypted, giving the name, address and telephone number of Brain Computer Services in Pakistan. The virus is copyright by "ashar and ashars", so we have two brothers running a computer store who have written a virus. Simple, right?

(Oh, the danger of simple answers.)

First of all, Alan Solomon's analysis and contention that ashar is older than Brain is quite convincing. Also, in the **most** common version of Brain, the address text does not appear. Further, it would be a very simple matter to have overlaid the text in the ashar or Brain programs with the

address text.

What motive would the owners of Brain Computer Services have for the writing of a virus? One story is that they sell pirated software, a practice that is legal in Pakistan, but not in the United States. Therefore, the infected disks were sold to Americans in punishment for their use of pirated software. Unconvincing. The moral attitude seems quite contorted, Brain would have no reason to "punish" the United States (its major source of software) and the Brain infection is not limited to the western world.

Another story is that Brain wrote some software of their own, and were incensed when others pirated **their** software. Unlikely. Infected disks would be most likely to be sold by Brain Computer Services, and this would tend to mean that a customer would be more likely to get a "clean" copy if it was pirated. (The hypothesis that Brain is some kind of copyright device is absurd: the virus would then be going around "legitimizing" bootleg copies.)

Given that Brain is relatively harmless it is possible that the virus was seen as a form of advertising for the company. Remember that this is the earliest known MS-DOS virus, and that the hardened attitude against viral programs had not yet arisen. Brain predates both Lehigh and Jerusalem, but even some time after those two "destructive" infections viral programs were still seen as possibly neutral or even beneficial. In those early, innocent days, it is not impossible that the author saw a self-reproducing program which "lost", at most, 3k of disk space as simply a cute gimmick.

I have mentioned Alan Solomon's analysis of the Brain family with regard to the dating of the ashar variant. Fridrik Skulason performed a similar analysis of the Ohio and Den Zuk versions, and has been proven 100% correct in his conclusions.

The Ohio and Den Zuk variants contain the Brain identification code, and so will not be "infected" or overlaid

by Brain. However, Ohio and Den Zuk identify Brain infections, and will replace Brain infections with themselves. Thus, Ohio and Den Zuk may be said to be agents acting against the Brain virus (at the expense, however, of having the Ohio and Den Zuk infections). frisk also found that the Den Zuk version preferentially overlaid Ohio. (This "seeking" activity gives rise to one of Den Zuk's aliases: "Search". It was also suspected that "denzuko" might have referred to "the search" for Brain infections. This turned out not to be the case.)

There is text in both strains which indicates a similarity of authorship. Ohio contains an address in Indonesia, both contain a ham radio licence number issued in Indonesia. Both contain the identical bug which overlays FAT and data areas on non-360K format disks. Den Zuk has the more sophisticated touches in programming. From all of this, frisk concluded that Ohio was, in fact, an earlier version of Den Zuk.

So it proved to be, in a message from the author. The author turns out to have been a college student in Indonesia who, to this day, sees nothing wrong with what he did. (On the contrary, he is inordinately proud of it, and is somewhat peeved that his earlier creation is "misnamed" Ohio: he's never been there. The name of Ohio was given by McAfee in reference to the place of the first identification of the viral program: Ohio State University.) Den Zuko is his nickname, derived from John Travolta's character in the movie "Grease".

Full details of Fridrik's analysis and his contact with the author are available in Fridrik's article in the Virus Bulletin.

Technically, the Brain family, although old, has a number of interesting points.

Brain itself is the first known MS-DOS virus, aside from those written by Fred Cohen for his thesis. In opposition to his, Brain is a boot sector infector. One wonders, given the fact

that the two earliest viral programs (for the Apple II family) were "system" viri [viruses], whether there was not some influence from these earlier, and similar, programs.

Brain is the first example of "stealth" technology. Not, perhaps, as fully armoured as other, later, programs, but impressive nonetheless. The intercepting and redirection of the system interrupts had to be limited in order for the virus to determine, itself, whether or not a target was infected.

The Den Zuk and Ohio variants use the trapping technology which can be used to have a virus survive a warm boot. Although they do not survive, the fact that the <Ctrl><Alt><Del> key sequence is trapped, and that another piece of programming (in this case, the onscreen display) is substituted for the reboot code proves the point. The virus could be made to survive and to "fake" a reboot. (The recovery of the system would likely require a lot of programming and code. This has been pointed out before, and the "recovery mode" of Windows 3.1 probably proves it.)

Den Zuk and Ohio are also "virus hunting viri [viruses]". This possibility has long been discussed, and these examples prove it can be done. They also indicate that it is not a good idea: Den Zuk and Ohio are far more dangerous than Brain ever was.

The Solomon and Skulason analyses are fascinating for tracking the trail of a virus "mutation" through the same, and different, authors. The evolution of programming sophistication, the hesitation to alter the length of text strings, even while they are being replaced, and the retention and addition of bugs form an engrossing pattern to follow.

[Finally, a look at the Macintosh MacMag virus…](#)

Please visit our sponsors.

Dr. Solomon's History | | | 1986-1987 | 1988 | 1989 | 1990 | 1991 | 1992 | 1993 | The Future
Robert Slade's History | | | Earliest Virus History | Early Related | Fred Cohen | Pranks/Trojans | Apple Virus | Lehigh/Jerusalem |
(c) Brain | MacMag
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

---

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Robert Slade History

Virus Tutorial

Navigation

History Detail

Tutorial Map

Anti-Virus Software

MacMag virus

On February 7, 1988, users of Compuserve's Hypercard Forum were greeted with an intriguing warning message. It told them that the NEWAPP.STK Hypercard stack file was no longer on the system. The notice suggested that if they had downloaded the file, they should not use it. If they had used it, they should isolate the system the file had run on.

The story, on Compuserve, had actually started a day earlier. A user had earlier downloaded the same Hypercard stack from the Genie system, and noticed, when he used it, that an INIT resource had been copied into his system folder. (In the Mac world, this generally means that a program is executed upon startup. Many of these programs are "background" utilities which remain active during the course of the session.) The user, noticing that this same file was posted on Compuserve, had put up a warning that this file was not to be trusted.

The moderator of the Forum initially downplayed the warning. He stated that there was no danger of any such activity, since Hypercard "stacks" are data files, rather than programs. Fortunately, the moderator did check out the warning, and found that everything happened as the user had said. Furthermore, the INIT resource was "viral": it spread to other "systems" that it came in contact with. (At

that time "system" disks were more common among Mac users, as "bootable" disks were among MS-DOS users.) The moderator apologized, posted the warning, and a number of people started looking into the structure of the virus.

The virus appeared to be benign. It attempted to reproduce until March 2, 1988. When an infected computer was booted on that date, the virus would activate a message that "RICHARD BRANDOW, publisher of *MacMag*, and its entire staff would like to take this opportunity to convey their UNIVERSAL MESSAGE OF PEACE to all Macintosh users around the world." A laudable sentiment, perhaps, although the means of distribution was unlikely to promote a "peaceful, easy feeling" among the targeted community. Fortunately, on March 3 the message would appear once and then the virus would erase itself.

Authorship

Richard Brandow was the publisher and editor of the *MacMag* computer magazine. Based out of Montreal, it was reported at the time to have a circulation of about 40,000. An electronic bulletin board was also run in conjunction with the magazine.

Brandow at one point said that he had been thinking about the "message" for two years prior to releasing it. (Interesting, in view of the fact that the date selected as a "trigger", March 2, 1988, was the first anniversary of the introduction of the Macintosh II line. It is also interesting that a "bug" in the virus which caused system crashes affected only the Mac II.) Confronted by users upset by the virus, Brandow never denied it. Indeed, he was proud to claim "authorship", in spite of the fact that he did not, himself, write the virus. (Brandow had commissioned the programming of the virus, and internal structure contains the name "Drew Davidson".)

Brandow gave various reasons at various times for the writing of the virus. He once stated that he wanted to make

a statement about piracy and copying of computer programs. (As stated before in association with the Brain virus, a viral program can have little to do with piracy per se, since the virus will spread on its own.) However, most often he simply stated that the virus was a "message", and seemed to imply that somehow it would promote world peace. When challenged by those who had found and disassembled the virus that this was not an impressively friendly action, Brandow tended to fall back on rather irrational arguments concerning the excessive level of handgun ownership in the United States. (My apologies on behalf of my countrymen. While few of us like handguns, not many of us show this level of illogic.)

(It is interesting, in view of the "Dutch Crackers" group, the Chaos Computer Club and the Bulgarian "virus factory", that Brandow apparently felt he had a lot of support from those who had seen the virus in Europe. The level of social acceptance of cracking and virus writing shows an intriguing cultural difference between the European states and the United States.)

My suspicion, once again, is that the MacMag virus was written primarily with advertising in mind. Although it backfired almost immediately, Richard Brandow seems to have milked it for all it was worth, in terms of notoriety. For a time, in fact, he was the "computer commentator" for the CBC's national mid-morning radio show, "Morningside" (somewhat of an institution in Canada.) While I never heard of *MacMag* before the virus, I've never seen a copy since, either. According to the recent news reports, Richard Brandow now writes for "Star Trek".

Spread

Brandow claims to have infected two computers in MacMag's offices in December of 1987 in order to "seed" the infection. It probably isn't beyond the bounds of possibility that a few deliberately infected disks were distributed as well.

A resource (named DREW in the Hypercard stack and DR in its viral form) was copied into the System folder on Mac systems. The System folder, as the name implies, is the "residence" of the operating system files. With the resource based structure of the Mac OS, the operating system can be configured and customized by "dropping" resources into the System folder. (MS-DOS users, tired of fiddling with entries in CONFIG.SYS, conflicting TSRs and the like, might be warned that this does not always work as easily as it sounds.)

"Bootable" Mac disks contained a System folder, in the same way that "bootable" MS-DOS disks contain the "hidden" system files and COMMAND.COM. In those days, "system" disks were much more common than they are now. In addition, Mac users would often create "system" disks that would have specialized configurations. (I well remember, at the time, a number of Macintosh programs which would work with one specific version of the Finder only. This would put the user in the position of having to "downgrade" the computer each time it was desired to run these programs.) The Mac OS "opens" each disk inserted into the machine. Therefore, on an infected machine, any diskette which was inserted into the drive would have the MacMag virus into the system folder.

The MacMag viral resource was placed into the folder as an "INIT". This meant that it would be one of the "initial" programs automatically run on system startup. Many, if not most, INITs are background or resident programs which either monitor or support different functions on an ongoing basis. Therefore, this was a perfect position for a virus. On an ongoing basis it would be able to watch for opportunities to spread.

The MacMag virus was not a sophisticated piece of programming. As one of the earliest (one of the (rarely used) names for it was the "Macinvirus") Mac viral programs, it didn't have to be. (Some would say that Mac viri [viruses] don't have to be sophisticated anyway. Although the Mac

world have far fewer viral strains than does the MS-DOS world, infection rates of a given virus have tended to be far higher in Mac populations.) There is no particular secrecy to the MacMag virus. Anyone who looked could find it. Few, however, looked.

Thank you Mr. Slade.

That concludes the history section.

Virus protection… Next

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Pray the Rosary for peace.

ckNOW.com

Protection From Viruses

Virus Tutorial

Scanning

> **Scanning looks for known viruses by a signature or characteristics that make new viruses similar to existing viruses. This requires that anti-virus makers and users keep products up to date.**

Navigation

Virus Protection

Tutorial Map

Anti-Virus Software

Once a virus has been detected, it is possible to write scanning programs that look for telltale code (signature strings) characteristic of the virus. The writers of the scanner extract identifying strings from the virus. The scanner uses these signature strings to search memory, files, and system sectors. If the scanner finds a match, it announces that it has found a virus. This obviously detects only known, pre-existing, viruses. Many so-called "virus writers" create "new" viruses by modifying existing viruses. This takes only a few minutes but creates what appears to be a new virus. It happens all too often that these changes are simply to fool the scanners. (Please use the above as "concept" information. Writing a scanner today is quite a bit more complex.)

Note: Newer scanners often employ several detection techniques in addition to signature recognition. Among the most common of these is a form of code analysis. The scanner will actually examine the code at various locations in an executable file and look for code characteristic of a virus (e.g., a jump to a non-standard location, etc.). A second possibility is that the scanner will set up a virtual computer in RAM and actually test programs by running them in this virtual space and observing what they do. These techniques are often lumped under the general name "heuristic" scanning. Such scanners may also key off of code fragments that appear similar to, but not exactly the same as, known viruses.

The major advantage of scanners is that they allow you to check programs before they are executed. Scanners provide the easiest way to check new software for known or suspected viruses. Since they have been aggressively marketed and since they provide what appears to be a simple painless solution to viruses, scanners are the most widely-used anti-virus product.

Too many people seem to regard "anti-virus product" and "scanner" as synonymous terms. The peril here is that if too many people depend solely upon scanners, newly created viruses will spread totally unhindered causing considerable damage before the scanners catch up with the viruses. An example of this was the attack by the Maltese Amoeba

(Irish) virus in the UK. This virus was not detected prior to its destructive activation on November 1, 1991. Prior to its attack, it had managed to spread quite widely and none of the existing (mostly scanner-based) products detected this virus.

According to the December 1991 Virus Bulletin:

> *Prior to November 2nd, 1991, no commercial or shareware scanner (of which VB has copies) detected the Maltese Amoeba virus. Tests showed that not ONE of the major commercial scanners in use … detected this virus.*

This indicates the potential hazard of depending upon scanner technology for complete virus protection. (More recent examples have been fast-spreading viruses that also act like worms [e.g., Melissa]. Anti-virus software makers react rapidly to these threats but there is still some delay and users have to be constantly alert.)

Another major drawback to scanners is that it's dangerous to depend upon an old scanner. With the dramatic increase in the number of viruses appearing, it's risky to depend upon anything other than the most current scanner. Even that scanner is necessarily a step behind the latest crop of viruses since there's a lot that has to happen before the scanner is ready:

- The virus has to be detected somehow to begin with. Since the existing scanners won't detect the new virus, it will have some time to spread before someone detects it by other means.
- The newly-discovered virus must be sent to programmers to analyze and extract a suitable signature string or detection algorithm. This must then be tested for false positives on legitimate programs.
- The "string" must then be incorporated into the next release of the virus scanner.
- The virus scanner or detection database must be distributed to the customer.

In the case of retail software, the software must be sent to be packaged, to the distributors, and then on to the retail outlets. Commercial retail software takes so long to get to the shelves, that it is almost certainly out of date. Virtually all product makers today provide some way to obtain updates via the Internet in order to help speed up the update process.

If you depend upon a scanner, be sure to get the latest version directly from the maker. Also, be sure that you boot from a clean write-protected copy of DOS before running the scanner for the first time at least; there's a good chance that the scanner can detect a resident virus in memory, but if it misses the virus in memory, the scanner will wind up spreading the virus rather than detecting it. Every susceptible program on your disk could be infected in a matter of minutes this way! (See Fast and Slow Infectors.)

Ghost Positives

One possible defect of scanners you might run into are termed "ghost" positives.

When DOS/Windows reads from a disk it does not read exactly what is requested; it also reads a bit ahead so that when the next read request comes in DOS may just have the material needed in a memory buffer and it can be provided much faster. Likewise, when a scanner reads files it has to compare each with the detection database. These are stored

in memory.

If, after scanning, the scanner does not clear its buffers in memory and you immediately run a second scanner then the second scanner may see the first scanner's strings in memory and if it uses the same string(s) could identify that virus as being in memory.

This is why it's important to run your scanner (or other anti-virus product) after a cold boot. One of the features of a cold boot is a complete memory check and this check overwrites all of memory, clearing out all false traces of viruses.

False Alarms

Despite the most extensive testing it is possible that a scanner will present false alarms (i.e., indicate a file as infected when it really is not). You will usually note this just after an update where a file you've had on your system suddenly shows up as infected. If it's a single file, previously clean, that exhibits this characteristic you can rest a bit easier; but you should nevertheless check with your anti-virus software maker.

Testing a Scanner

You don't need a virus to test the installation of a scanner. Most good scanners today are programmed to detect a standard test file called the EICAR test file. You can easily make this test file. Simply type or copy the following string into a text editor like Notepad:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Now save that file under the name EICAR.COM. This is an actual program that, when run, will display the text EICAR-STANDARD-ANTIVIRUS-TEST-FILE! and, when scanned, should activate your anti-virus program.

Note: This is not a virus. It is simply a file designed to activate the detection routines in scanners that support it. (Some suggest you need a "good" virus to test scanners. The problem is that to adequately test a scanner you need a virus "zoo" and have to install each virus in the zoo and test against it. This is something few users would want to do. The EICAR test file tests the installation of anti-virus software and that should be sufficient.)

Summary

- Scanning depends on prior knowledge of a virus in order to detect it. This is done by recognizing some sort of signature that represents the virus or some program characteristic that indicates a virus may be present.
- Scanners allow you to check programs before execution. That is their main advantage.
- Scanners need to be regularly updated. Don't depend on an old scanner.
- Some viruses attempt to defeat scanners by changing their code on the fly. Current scanners attempt to analyze code on the fly as a way of countering this.
- Never run two scanners in a row without cold booting to clear memory between. If you do, you may find "ghost" positives.

Let's now look at integrity checking…

Please visit our sponsors.

Click Here to Visit our Sponsor

Protection Intro | Scanning | Integrity Checking | Interception | AV Product Use | File Extensions | Safe Hex | Outlook vs. Outlook Express | Scripting | Backup | On-going Virus Info
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Protection From Viruses

Virus Tutorial

Navigation

Virus Protection

Tutorial Map

Anti-Virus Software

Integrity Checking

> **Integrity products record information about your system for later comparison in order to detect changes. Just detecting changes is not enough, however; the detection must have some "intelligence" behind it to avoid confusion.**

Integrity checking products work by reading your entire disk and recording integrity data that acts as a signature for the files and system sectors. An integrity check program with built-in intelligence is the only solution that can handle **all** the threats to your data as well as viruses. Integrity checkers also provide the only reliable way to discover what damage a virus has done.

So, why isn't everyone using an integrity checker? In fact, many anti-virus products now incorporate integrity checking techniques. One problem with many products is that they don't use these techniques in a comprehensive way. There are still too many things not being checked.

Some older integrity checkers were simply too slow or hard to use to be truly effective. A disadvantage of a bare-bones

integrity checker is that it can't differentiate file corruption caused by a bug from corruption caused by a virus.
Advanced integrity checkers that incorporate the capability to analyze the nature of the changes and recognize changes caused by a virus have become available. Some integrity checkers now use other anti-virus techniques along with integrity checking to improve their intelligence and ease of use.

If you choose an integrity checker, be sure it has all these features:

- It's easy to use with clear, unambiguous reports and built-in help.
- It hides complexity, so that complicated details of system file or system sector changes are only presented if they contain information the user must act upon.
- The product recognizes the various files on the PC so it can alert the user with special warnings if vital files have changed.
- It's fast. An integrity checker is of no use if it's too slow.
- It recognizes known viruses, so the user doesn't have to do all the work to determine if a change is due to a software conflict, or if it's due to a virus. This also helps protect the integrity checker against attacks by viruses directed at it.
- It's important that the integrity computation be more sophisticated than a mere checksum. Two sectors may get reversed in a file or other damage may occur that otherwise rearranges data in a file. A simple checksum will not detect these changes. A cryptographic computation technique is best.
- It's comprehensive. Some integrity checkers, in order to improve their speed, don't read each file in its entirety. They read only portions of larger files. They just spot check. This is unacceptable; it's important to know the file hasn't changed, not just that some of the file hasn't changed.

- It checks and restores both boot and partition sectors. Some programs check only files.
- For protection, it should have safety features built in (e.g., ability to define the signature information file name and store the information on a floppy disks).

While using an integrity checker is an excellent way to monitor changes to your system, with today's operating systems so many files change on a regular basis it's imperative that you also use a good up-to-date scanner along with the integrity checker or for the integrity checker to have that capability built in.

Summary

- Integrity checking products read the disk and create signature information to determine changes.
- Coupled with virus identification, using integrity checking should be able to detect most any virus with the bonus of also detecting data corruption.

[Interception is the third AV type](#)…

Please visit our sponsors.

[Click Here to Visit our Sponsor](#)

[Protection Intro](#) | [Scanning](#) | [Integrity Checking](#) | [Interception](#) | [AV Product Use](#) | [File Extensions](#) | [Safe Hex](#) | [Outlook vs. Outlook Express](#) | [Scripting](#) | [Backup](#) | [On-going Virus Info](#)
[Virus Tutorial Home](#) | [Virus Intro](#) | [Virus Types](#) | [Virus History](#) | [Virus Protection](#) | [Virus Hoaxes](#) | [Current Threats](#)
[Home](#) | [Products](#) | [Definitions](#) | [Newsletter](#) | [Virus Tutorial](#) | [Contact](#)

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Send mail to webmaster@cknow.com with questions or comments about this web site.

[Pray the Rosary](#) for peace.

cknow.com

Protection From Viruses

Virus Tutorial

Navigation

Virus Protection

Tutorial Map

Anti-Virus Software

Interception

> Monitoring for system-level routines that perform destructive acts can help, but such monitoring is fairly easily bypassed. Do not depend on it alone.

Interceptors (also known as resident monitors) are particularly useful for deflecting logic bombs and Trojans. The interceptor monitors operating system requests that write to disk or do other things that the program considers threatening (such as installing itself as a resident program). If it finds such a request, the interceptor generally pops up and asks you if you want to allow the request to continue. There is, however, no reliable way to intercept direct branches into low level code or to intercept direct input and output instructions done by the virus itself. Some viruses even manage to disable the monitoring program itself. Indeed, for one widely-distributed anti-virus program several years back it only took eight bytes of code to turn its monitoring functions off.

It is important to realize that monitoring is a risky technique. Some products that use this technique are so annoying to use (due to their frequent messages popping up)

that some users consider the cure worse than the disease!

Summary

- Interceptors are useful for some simple logic bombs and Trojans.
- It would be unwise to depend entirely upon behavior monitors as they are easily bypassed.

AV Product Use Guidelines…

Protection Intro | Scanning | Integrity Checking | Interception | AV Product Use | File Extensions | Safe Hex | Outlook vs. Outlook Express | Scripting | Backup | On-going Virus Info
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Pray the Rosary for peace.

cknow.com

Protection From Viruses

Virus Tutorial

Navigation

Virus Protection

Tutorial Map

Anti-Virus Software

AV Product Use Guidelines

> **First, understand how your anti-virus product works. Then, start with a known-clean computer and follow specific steps to assure good virus detection/protection. Do research on specific products before purchase.**

Most modern anti-virus products use a combination of techniques. However, they still get almost all of their protection from their scanner component. It's vital to understand exactly how your product works so that you understand what type of protection you really have (you might want to review the comments about scanning, interception, and integrity checking on other tutorial pages). Here are some rules that will help you make sure that you get maximum protection out of whatever product you have:

- First, you should check your computer's setup information to make certain that the boot sequence starts with the floppy drive. If you don't, and it starts with the hard drive then any boot sector virus on your computer will gain control before you run the anti-

virus program(s). To get to the BIOS setup you will typically have to press a key or keystroke combination during the time the BIOS is checking the computer's memory. Once in setup you can check the boot sequence (one of the techniques used to protect against boot sector viruses on floppy disks is to set the boot sequence to check the hard drive first--but if this is set then you won't be able to boot from a clean floppy as indicated below; thus, this check).

- Be sure to cold boot your PC from a write-protected diskette before virus checking, particularly if you suspect you have a virus. Most anti-virus products make this recommendation, but this rarely gets done because the recommendation is often buried in some obscure location in the documentation. If your PC's memory is infected with a virus that your scanner does not recognize, you could infect all the programs on your disk if you do not boot from a clean disk. Don't take this chance; boot from a write-protected diskette before you scan. (In some cases, the AV product might come with a bootable CD-ROM instead. If so, then set the BIOS default to boot from the CD and use that disc.)

- If you are using a product which depends mostly on its scanner component, make sure that you always have the latest version. Scanners are often frequently updated (one AV program vendor says they update files on the Internet hourly if needed).

- Before you execute or install any new software, check it first (yes, commercial software has come from the factory infected). If it comes with an install program, check again after you install the software; an install program will frequently change or decompress executable programs. After you first execute brand new software do an additional check of your system to make sure everything is as it should be.

- If your product contains a scanner component, check all diskettes brought in from another location; even data diskettes! Inevitably someone will leave a data diskette in their A: drive, potentially spreading a boot

sector virus if the diskette is infected (assuming you have not reset the boot sequence back to booting from the hard disk first).

- If the anti-virus software has a component that installs under Windows in order to scan all files before they are opened by all means install that component. This is a valuable service that is well worth the small amount of slowdown and resource use you will experience.

What's the best anti-virus product?

The simple answer is that there is no definite answer to the question! For one thing, a "good" anti-virus product integrates well with your particular system and system setup. If you are on a network with diskless workstations, for example, you might want to install the anti-virus software on the server. If you don't regularly exchange or download files you might find a less intrusive anti-virus product more to your liking. And so on.

Relying on magazine articles is also not the best way to decide upon an anti-virus product. Valid testing requires special setups to make certain products are being tested against real viruses under conditions those viruses might be found (e.g., it would not be a particularly useful test to place boot sector viruses into zip archives and then testing an anti-virus product against that archive).

One measure of anti-virus software is ICSA approval. To obtain this approval a scanner must detect all viruses on the current version of the Wild List in addition to 90% of the full NCSA test suite. You can obtain more information about this at:

http://www.icsa.net/services/product_cert/

If you want to try an anti-virus product, many producers have evaluation versions at their web site.

Summary

- Understand your anti-virus product and what you can expect from it.
- Check setup to be certain you are booting from the floppy disk and then cold boot from a known-clean, write-protected diskette.
- Scan only with the latest version of any scanner.
- Check all new software and all data diskettes before use and again after the installation.
- Install any scan-on-use component your anti-virus product may have.
- Do a bit of research and look for certification when you purchase anti-virus software.

[Should you depend on file extensions](#)?… Next

Protection Intro | Scanning | Integrity Checking | Interception | AV Product Use | File Extensions | Safe Hex | Outlook vs. Outlook Express | Scripting | Backup | On-going Virus Info
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Pray the Rosary for peace.

ckNOW.com

Protection From Viruses

Virus Tutorial

File Extensions

Navigation

Virus Protection

[Tutorial Map](#)

[Anti-Virus Software](#)

> There is currently a big push toward relying heavily on recognizing "bad" file extensions and acting solely on this knowledge. That's not necessarily a good thing as extensions can be misleading.

One of the most asked questions lately is "What extensions should I scan and/or watch for in E-mail attachments?" While a valid question, some caveats must be attached to the answer.

First, it's important to note that over time Microsoft (and others) appear to be working toward making file extensions as the sole indicator of file content and creator unnecessary. This already exists on the Macintosh where the file creator information is in the file itself so the file name and extension is no indicator at all of the type of file.

Such behavior is starting to appear under Windows as well. Microsoft Word, for example, will actually examine a file it's asked to open and, despite the name ending in .DOC, if the file is a template file will open the file as a template (.DOT) file instead. Some Word macro viruses take advantage of this characteristic and save infected files in template format with a .DOC extension.

Another variant of this behavior on Windows computers would be the Scrap Object file which actually can contain most anything from simple text to complex programs. When opened, the operating system determines what the content is and acts accordingly.

Finally, there is the issue of double extensions. To make your viewing

easier, Windows offers the option of turning off the viewing of file extensions. If you do that, however, you can easily be fooled by files with double extensions. Most everyone has been conditioned, for example, that the extension .TXT is safe as it indicates a pure text file. But, with extensions turned off if someone sends you a file named BAD.TXT.VBS you will only see BAD.TXT. If you've forgotten that extensions are actually turned off you might think this is a text file and open it. Instead, this is really an executable VisualBasic Script file and could do serious damage. For now you should always have viewing extensions turned on. Here's how…

In Windows 98 double click to open "My Computer" and then select "View"|"Folder Options". Select the "View" tab and then scroll down to the entry that says "Hide file extensions for known file types" and make certain it's not checked. Click OK and then close the My Computer window. With this move you will now see extensions in file directory windows and the option will be picked up by other Microsoft programs like Outlook.
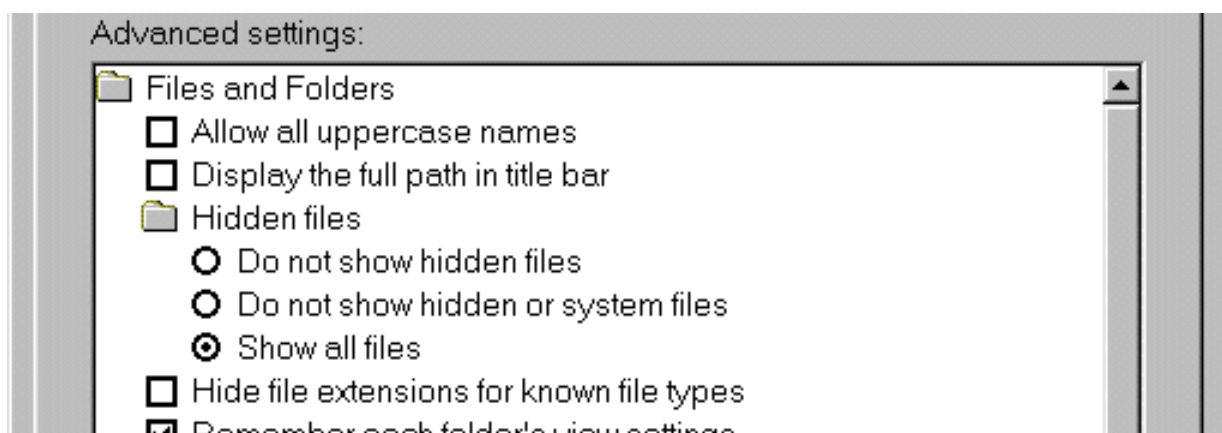
Extensions

So, with the thought in mind that file extensions are likely being phased out over time and can be spoofed, here are some to watch out for ("?" represents any character):

.386	**Windows Enhanced Mode Driver.** A device driver is executable code and, as such, can be infected and should be scanned.
.ADE	**Microsoft Access Project Extension.** Use of macros makes this vulnerable.
.ADP	**Microsoft Access Project.** Use of macros makes this vulnerable.

.ADT	**Abstract Data Type**. According to Symantec these are database-related program files.
.APP	**Application File**. Associated with a variety of programs; these files interact with such things as database programs to make them look like standalone programs.
.ASP	**Active Server Page**. Combination program and HTML code.
.BAS	**Microsoft Visual Basic Class Module**. These are programs.
.BAT	**Batch File**. These are text files that contain system commands. There have been a few batch file viruses but they are not common.
.BIN	**Binary File**. Can be used for a variety of tasks and usually associated with a program. Like an overlay file it's possible to infect .BIN files but not usually likely.
.BTM	**4DOS Batch To Memory Batch File**. Batch file that could be infected.
.CBT	**Computer Based Training**. It's never been made clear why or how these can become infected but Symantec includes them in their default listing.
.CHM	**Compiled HTML Help File**. Use of scripting makes these vulnerable.
.CLA .CLASS	**Java Class File**. Java applets are supposed to be run in a "sandbox" and thus be isolated from the system. However, users can be tricked into running an applet in a mode that the sandbox considers "secure" so Class files should be scanned.
.CMD	**Windows NT Command Script**. A batch file for NT.
.COM	**Command (Executable File)**. Any executable file can be infected in a variety of ways.
.CPL	**Control Panel Extension**. Similar to a device driver which is executable code and, as such, can be infected and should be scanned.

.CRT	**Security Certificate.** Can have code associated with it.
.CSC	**Corel Script File.** A type of script file that is executable. Any executable should be scanned.
.CSS	**Hypertext Cascading Style Sheet.** Style sheets can contain code.
.DLL	**Dynamic Link Library.** Can be used for a variety of tasks associated with a program. DLLs typically add functions to programs. Some contain executable code; others simply contain functions or data but you can't tell by looking so all DLLs should be scanned.
.DOC	**MS Word Document.** Word documents can contain macros that are powerful enough to be used for viruses and worms.
.DOT	**MS Word Document Template.** Word templates can contain macros that are powerful enough to be used for viruses and worms.
.DRV	**Device Driver.** A device driver is executable code and, as such, can be infected and should be scanned.
.EML or .EMAIL	**MS Outlook Express E-mail.** E-mail messages can contain HTML and scripts. Many viruses and worms use this vector.
.EXE	**Executable File.** Any executable file can be infected in a variety of ways.
.FON	**Font.** Believe it or not, a font file can have executable code in it and therefore can be infected.
.HLP	**Help File.** Help files can contain macros. They are not a common vector but have housed a Trojan or two.
.HTA	**HTML Program.** Can contain scripts.
.HTM .HTML	**Hypertext Markup Language.** HTML files can contain scripts which are more and more becoming vectors.

.INF	**Setup Information.** Setup scripts can be changed to do unexpected things.
.INI	**Initialization File.** Contains program options.
.INS	**Internet Naming Service.** Can be changed to point unexpected places.
.ISP	**Internet Communication Settings.** Can be changed to point unexpected things.
.JS .JSE	**JavaScript.** As script files become vectors more often it's best to scan them. (.JSE is encoded. Also keep in mind that these can have other, random, extensions!)
.LIB	**Library.** In theory, these files could be infected but to date no LIB-file virus has been identified.
.LNK	**Link.** Can be changed to point to unexpected places.
.MDB	**MS Access Database** or **MS Access Application.** Access files can contain macros that are powerful enough to be used for viruses and worms.
.MDE	**Microsoft Access MDE database.** Macros and scripts make this vulnerable.
.MHT .MHTM .MHTML	**MHTML Document.** This is an archived Web page. As such it can contain scripts which can be infected.
.MP3	**MP3 Program.** While actual music files cannot be infected, files with .mp3 extensions can contain macro code that the Windows or RealNetwork media players will interpret and run. So, .mp3 files have expanded beyond pure music.
.MSO	**Math Script Object.** According to Symantec these are database-related program files.
.MSC	**Microsoft Common Console Document.** Can be changed to point to unexpected places.
.MSI	**Microsoft Windows Installer Package.** Contains code.

.MSP	**Microsoft Windows Installer Patch.** Contains code.
.MST	**Microsoft Visual Test Source Files.** Source can be changed.
.OBJ	**Relocatable Object Code.** Files associated with programs.
.OCX	**Object Linking and Embedding (OLE) Control Extension.** A program that can be downloaded from a Web page.
.OV?	**Program File Overlay.** Can be used for a variety of tasks associated with a program. Overlays typically add functions to programs. It's possible to infect overlay files but not usually likely.
.PCD	**Photo CD MS Compiled Script.** Scripts are vulnerable.
.PGM	**Program File.** Associated with a variety of programs; these files interact with such things as database programs to make them look like standalone programs.
.PIF	**MS-DOS Shortcut.** If changed can run unexpected programs.
.PPT	**MS PowerPoint Presentation.** PowerPoint presentations can contain macros that are powerful enough to be used for viruses and worms.
.PRC	**Palmpilot Resource File.** A PDA program (yes, there are rare PDA viruses).
.REG	**Registry Entries.** If run these change the registry.
.RTF	**Rich Text Format.** A format for transmitting formatted text usually assumed to be safe. Binary (and infected) objects can be embedded within RTF files, however, so, to be safe, they should be scanned. RTF files can also be DOC files renamed and Word will open them as DOC files.

.SCR	**Screen Saver** or **Script**. Screen savers and scripts are both executable code. As such either may contain a virus or be used to house a worm or Trojan.
.SCT	**Windows Script Component**. Scripts can be infected.
.SHB .SHS	**Shell Scrap Object File**. A scrap file can contain just about anything from a simple text file to a powerful executable program. They should generally be avoided if one is sent to you but are routinely used by the operating system on any single system.
.SMM	**Ami Pro Macro**. Rare, but can be infected.
Source	**Source Code**. These are program files that could be infected by a source code virus (these are rare). Unless you are a programmer these likely won't be a concern. Extensions include, but are not limited to: .ASM, .C, .CPP, .PAS, .BAS, .FOR.
.SYS	**System Device Driver**. A device driver is executable code and, as such, can be infected and should be scanned.
.URL	**Internet Shortcut**. Can send you to any unexpected Web location.
.VB .VBE	**VBScript File**. Scripts can be infected. (.VBE is encoded.)
.VBS	**Visual Basic Script**. A script file may contain a virus or be used to house a worm or Trojan.
.VXD	**Virtual Device Driver**. A device driver is executable code and, as such, can be infected and should be scanned.
.WSC	**Windows Script Component**. Scripts can be infected.
.WSF	**Windows Script File**. Scripts can be infected.
.WSH	**Windows Script Host Settings File**. Settings can be changed to do unexpected things.

.XL?	**MS Excel File.** Excel worksheets can contain macros that are powerful enough to be used for viruses and worms.

The above listing has been derived from the default extension lists of various anti-virus programs and from discussions in virus-related newsgroups. It should not be taken as an absolute however. Some viruses/worms have been spread in files with no extension and, as noted, an extension does not necessarily guarantee a particular file type. The meaning for extensions not listed here might be found at http://filext.com/.

The safe option is to allow anti-virus software to scan all files.

Summary

- While extensions are often touted as being accurate indicators of files that can be infected, history shows they are not. Additionally, they can be spoofed in a variety of ways.
- The safe option is to allow anti-virus software to scan all files.

Let's look at how to practice safe hex…

Please visit our sponsors.

Click Here to Visit our Sponsor

Send mail to webmaster@cknow.com with questions or comments about this web site.
Pray the Rosary for peace.

ckNOW.com

Protection From Viruses

Virus Tutorial

Navigation

Virus Protection

Tutorial Map

Anti-Virus Software

Safe Computing Practices (Safe Hex)

> There are some relatively simple things you can do to help protect yourself from viruses and worms. Consider those listed on this page.

There are some common sense things you can do to help protect yourself against viruses and worms.

- **Update AV Software.** Obviously, the first and foremost save computing practice would be to make certain you keep your anti-virus software up to date. Do this at least weekly; more often if there are news reports of a new fast-spreading virus or worm.
- **Safe Boot Disk.** Most anti-virus software has an option for creating a safe boot disk which can be used to clean-boot the computer and, perhaps, also scan for viruses. This safe boot disk should be recreated now and again if it allows for virus scanning. It's important that it contains the latest virus database.
- **Hard Disk Boot.** Change your boot sequence so that the hard disk is the first boot disk instead of the floppy disk. It's really easy to leave a floppy disk in the

drive and if that disk happens to be infected with a boot sector virus then the next time you start the computer the hard disk will become infected. If the floppy is not accessed, that infection won't take place. The boot sequence is changed in your BIOS setup information and can be switched back when you need to boot from a floppy disk.

- **Use RTF Not DOC.** Don't accept any Word .DOC or Excel .XLS files from anyone. If you absolutely need formatted text to edit tell people to send you a Rich Text Format (.RTF) file. But, be careful none-the-less. There are macro viruses that intercept the request to save to RTF and save the file in DOC format with an RTF extension. Word will unfortunately ignore the RTF extension and open the file as a DOC file. To be certain, you can open the RTF file in a plain text editor to make certain it's plain text, as an RTF file should be. It is also possible to embed objects into RTF files. These also could be malicious. RTF is not as safe as many make it out to be. If the file has to be formatted but does not need to be edited, consider asking for it in PDF format instead.

- **Consider Alternate Software.** In the politest sense this would be a recommendation to switch to software that is not as likely to be affected by viruses/worms. For many offices a switch away from Word, Excel, and Outlook/Outlook Express would be difficult as these programs came as standard software on many systems. But, it's worth consideration.

- **Don't Open Attachments.** Be picky and stubborn: do not accept, run, or open any unsolicited attachments to E-mail. This may seem a bit extreme but in today's world where worms send themselves out via personal address books you can't really trust anything coming from anyone; even if you know them.

- **Turn off Preview.** No matter what E-mail software you use, turn off the preview function. Most that preview formatted messages use IE components that have proven themselves less than secure.

- **Disable Scripting.** Turn off the Windows Scripting Host

if you don't need it. Scripts are just fancy macros that can apply across programs and are a major vehicle for worms. Instructions here.

- **Show Extensions**. Set all programs to show you the full file name, particularly E-mail programs. If your program drops the extension you don't really know if the attachment is executable or not.
- **Protect Floppies**. Write-protect any floppy disk you place into another person's computer. If their computer is infected with a boot sector virus at least yours won't be.
- **Keep Up**. Keep up with the latest security patches for all the programs you use.
- **Get Info**. Consider subscribing to the virus alert E-mail notices your anti-virus software maker probably puts out. This is a two-edged sword, however. Many people will find they are getting many notices about viruses that they'll never see. You have to judge the inconvenience versus the information.
- **Backup**. Finally, but most importantly: backup, backup,**backup**!

What about using Outlook Express?…

Please visit our sponsors.

Click Here to Visit our Sponsor

Protection Intro | Scanning | Integrity Checking | Interception | AV Product Use | File Extensions | Safe Hex | Outlook vs. Outlook Express | Scripting | Backup | On-going Virus Info
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

---

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.

[Pray the Rosary](#) for peace.

cknow.com

Protection From Viruses

Virus Tutorial

Navigation

Virus Protection

Tutorial Map

Anti-Virus Software

Outlook and Outlook Express

This page will hopefully clarify some of the noted confusion about the ability of Outlook and Outlook Express to interact with worms and viruses. In many ways it's a shame that Microsoft had to name the programs with such similar names. With different names the confusion that currently seems to exist would not.

Despite the similar names, Outlook and Outlook Express are two different programs with two different development histories.

The Outlook E-mail client was designed as a replacement for the mail clients MS Exchange and MS Mail. Basically, it's a shoehorn of an Internet mail client into the proprietary MS Mail/Exchange clients.

Outlook Express was a rewrite and expansion of the Internet Email and News client that came with early Internet Explorer browsers (version 3 at least, not certain about version 2).

While Outlook 97 is a full OLE (MS Automation) client and server it did not make methods for accessing the address book and sending mail available to external users (the external user was assumed to know the address it wanted to

send mail to). Apparently finding this too restrictive, Microsoft, in Outlook 98, made these interfaces available to external users to work with (i.e., the external user no longer needed to know an E-mail address, they could use addresses stored by Outlook). It's this change that makes it possible for Outlook 98 (and later) to be used by virus/worm authors to do their E-mail tasks for them.

There presently does not appear to be a way to use the Visual Basic Application language tools built into Outlook for macro virus purposes (as you can with Word and Excel) but future changes may allow this.

Outlook Express, unlike Outlook, does not presently make any of its mail routines available to MS Automation (at least in all present shipping versions--who knows what the future may bring).

So, in general, when you see a worm/virus description talk about "Outlook" you can generally assume it means the Outlook program and not the Outlook Express program.

But, as with everything, there is at least one (and in the future more?) caveat. The KAK worm specifically targets Outlook Express by changing the default signature to one containing JavaScript code that acts as a worm. (This is a special case where it appears the worm author was trying to "infect" a program that was not supposed to be able to be infected.)

Now let's see how to disable scripting… Next

Please visit our sponsors.

Click Here to Visit our Sponsor

Protection Intro | Scanning | Integrity Checking | Interception | AV Product Use | File Extensions | Safe Hex | Outlook vs. Outlook Express | Scripting | Backup | On-going Virus Info

---

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.

Pray the Rosary for peace.

cknow.com

Protection From Viruses

Virus Tutorial

Navigation

Virus Protection

Tutorial Map

Anti-Virus Software

Disable Scripting

> **The Windows Scripting Host is used by few but makes many avenues of mischief available to malicious software. Consider removing or deactivating it.**

In order to run VisualBasic Scripts (VBS files) on your computer you must have the Windows Scripting Host (WSH) installed and working on your computer. While scripting allows you to closely integrate some application software, it also allows worms such as LoveLetter (as one example) to use your copy of Outlook to send itself to all the people in your address book (and other malicious things!).

In order to avoid these sorts of attacks it's often best to just disable the Windows Scripting Host. Most people don't need/use it. Following are instructions for removing WHS.

Windows98

Typically, WSH is installed if you choose a standard install of the OS, if you install the IE5 browser, or if you directly install WSH from Microsoft. To turn it off…

- Open the Add/Remove Control Panel application. Either "Start | Settings | Control Panel" or double click "My Computer" and "Control Panel" then double click "Add/Remove Programs."
- Click on the "Windows Setup" tab.
- Scroll to "Accessories" and double click that entry. An accessories windows that looks like the following should open…
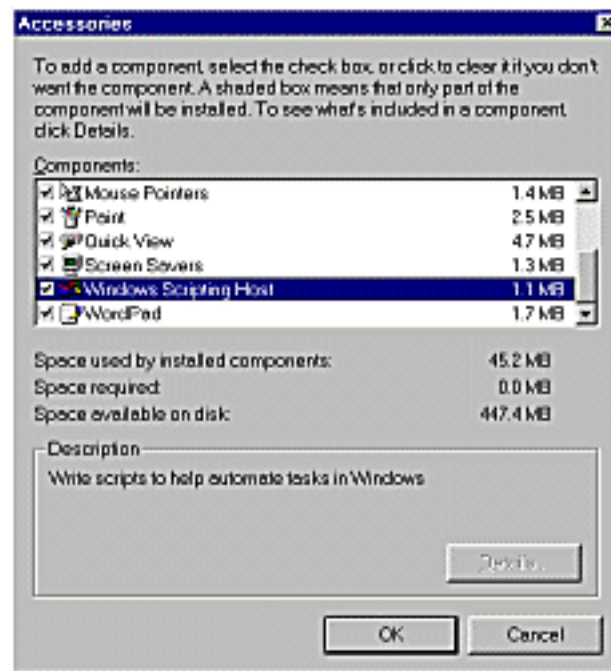
- Scroll down the accessories list until you find "Windows Scripting Host" and then click on the checkbox next to the entry to deselect it (i.e., remove the check mark in the box).
- Click OK to close the window(s) and OK again to close the "Add/Remove Programs" window.

(Windows 98 is the only OS Computer Knowledge has tried this process on. Following are brief instructions believed to work for other operating systems.)

Windows95

Basically, you have WSH installed if you've installed the IE5 browser or WSH itself. In order to stop it from running you have to disassociate the VBS extension with the WSH. Right

click "My Computer" on the Desktop or in Windows Explorer. Select "Open." Click on the "View" menu and select "Options…." Now click on the "File Types" tab. Scroll down to "VBScript Script File" (if not found stop here and cancel out; you don't have scripting active). Click on the "VBScript Script File" and select "Remove." Confirm and then quit the File Types application.

WindowsNT 4.0

Basically, you have WSH installed if you've installed the IE5 browser or WSH itself. In order to stop it from running you have to disassociate the VBS extension with the WSH. Log on as an administrator. Right click "My Computer" on the Desktop or in Windows Explorer. Select "Open." Click on the "View" menu and select "Options…." Now click on the "File Types" tab. Scroll down to "VBScript Script File" (if not found stop here and cancel out; you don't have scripting active). Click on the "VBScript Script File" and select "Remove." Confirm and then quit the File Types application.

Windows 2000

WSH is normally installed. In order to stop it from running you have to disassociate the VBS extension with the WSH. Log on as an administrator. Right click "My Computer" on the Desktop or in Windows Explorer. Select "Open." Click on the "View" menu and select "Options…." Now click on the "File Types" tab. Scroll down to "VBScript Script File" (if not found stop here and cancel out; you don't have scripting active). Click on the "VBScript Script File" and select "Remove." Confirm and then quit the File Types application.

Backups are important…

Please visit our sponsors.

[Click Here to Visit our Sponsor](#)

Protection Intro | Scanning | Integrity Checking | Interception | AV Product Use | File Extensions | Safe Hex | Outlook vs. Outlook Express | Scripting | Backup | On-going Virus Info
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

---

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Protection From Viruses

Virus Tutorial

Backup Strategy

Navigation

Virus Protection

Tutorial Map

Anti-Virus Software

> Once damage is done to files on your computer (no matter what the cause) it's often too late. A comprehensive backup strategy is a vital component in your computer security arsenal (and don't forget to test the restore routines!).

Too many people wait for a problem to happen or a virus to attack their PC before they take any action. Once a virus reveals its presence on your PC, it may be too late to recover damaged files. There are many viruses that cannot be successfully removed due to the way the virus infects the program. It's absolutely vital to have protection before the virus strikes. If you wait until you notice that your hard disk is losing data, you may already have hundreds of damaged files.

And, don't forget problems caused by hardware or software glitches. A good backup is excellent protection against those unscheduled events as well.

It's essential to carefully protect all your software and regularly back up the data on all your disks. Do you have a

single disk that you can afford not to regularly backup? It's rare to find any PC that does not have some type of important data stored on it (why would you store it if you at least didn't feel it was important at the time?).

Suggested Policy

- All original software (program) diskettes should immediately be write-protected, copied and stored in two secure, separate locations after installation. If you are using an integrity check program, immediately record (initialize) the integrity data for the new programs after installing. (Store CD-ROMs in a fire-secure location since you only have one copy of them.)
- Determine a schedule for full backups by considering how frequently your data changes. It is an excellent idea to have three full sets of backup tapes or data cartridges and to **store one set at another location** to protect against fire, theft, or some other disaster. If your data is critical, you may wish to have a separate cycle of backups (e.g., quarterly or yearly) that can be used to recover when someone damages (or deletes) a vital file, but the deletion isn't discovered until months later.
- The full backups should be coordinated with periodic incremental backups. The incremental backup, which copies just the files that have changed, normally runs very quickly and takes just a minute or so. Many people find that an incremental backup run at the end of each day works quite well. This way their data is protected should anything happen overnight. **One rule of thumb for incremental backups is to do them when it would become difficult or not cost effective to re-enter the data.**
- Make sure you use reliable backup hardware and software. Periodically test by **restoring from a backup**. Too many people have discovered that their backup program couldn't recover their files when it was too late. If you use an integrity check program you can verify that the restored files are correct. If you

cannot afford to play with your operational system, test your restore on a different system. This will also tell you if you will be able to restore to a new system should the current one have to be replaced.

- **Be certain you store the recovery program for your backups with your backups.** Some people have regularly backed up their data only to find the only version of the recovery program was on their backups and not available to actually run.

When you store your backup use great caution where you store it. Pick a place that will be safe as a physical location. Plan ahead for flood, for example. Don't store your backups in the basement if your business is next to a river! Plan ahead for fire; and if the location is protected by sprinklers what will the water do to the backups? What about physical access? And, so on.

Summary

- Plan for problems before they happen by having a good (and current) backup.
- Develop a backup strategy based on how much work you are willing to do to reenter information.
- Keep at least one backup copy off-site.
- Test your ability to restore from your backup before you have to and be certain to store the recovery program with the back.

That basically the end of the tutorial. Thank you for reading to this point. But, that's only the start of virus information…

On-going virus info…

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Protection From Viruses

Virus Tutorial

On-going Virus Information

> There are many sources for virus information; some are even accurate.

Navigation

Virus Protection

Tutorial Map

Anti-Virus Software

The first place to check often is the web site of your anti-virus provider. There you should find alerts for the latest viruses, information about using their product in the most efficient manner, and, of course, the latest updates. Often you will also find you can join a mailing list and receive upgrade and alert notices automatically via E-mail.

You can also check other anti-virus software vendor sites for their latest alerts and, if you have time and bandwidth to spare join their mailing lists as well. (The link to your left will direct you to a list of some anti-virus software vendors.)

Also, don't forget to check the Computer Knowledge site. Our monthly newsletter often has notes about new viruses and other security items you should be aware of.

http://www.cknow.com/cknewsletter/

There are several usenet newsgroups dedicated to computer viruses. Of these, comp.virus is the best largely because it is

moderated by virus experts so the trash postings are suppressed. Unfortunately, the moderator(s) have not been able to process messages very often and so the newsgroup has been quiet for a long time now. The alt.comp.virus newsgroup is quite active as an alternative but there are a considerable number of posts in the group that offer either no benefit or are just plain wrong. Use caution if you read alt.comp.virus or any of the other related alt groups.

There are many more sources of information listed in the alt.comp.virus FAQ. It's posted regularly to alt.comp.virus and comp.virus and is available on the web at:

> http://www.sherpasoft.com/acvFAQ/

Specific Virus Descriptions

Some anti-virus vendor sites have databases describing specific viruses in varying detail. Check the FAQ link just above for some links or check the AVP, Data Fellows, Symantec, and McAfee vendors sites (click on the anti-virus software link).

Different vendors sometimes have different names for the same virus. If you can't find a particular virus on one site, check another. You can also check the Virus GREP database which attempts to cross reference all the different virus names. See:

> http://www.virusbtn.com/VGrep/

Books

Books which may be of use (a few of these are somewhat dated but still of some value for learning the basics):
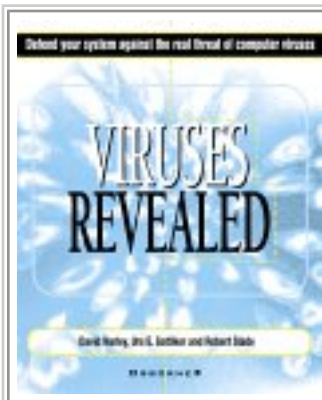
[Viruses Revealed](#)
by
David Harley, Urs E. Gattiker, Robert Slade
Paperback-400 pages (August 2001)
Osborne McGraw-Hill
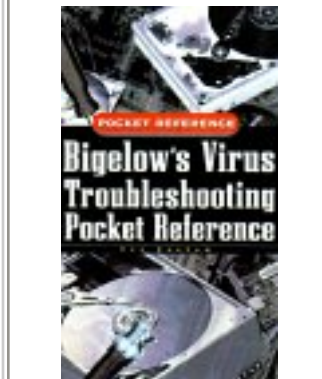
[Bigelow's Virus Troubleshooting Pocket Reference](#)
by
Ken Dunham
Paperback-267 pages 1st edition (August 7, 2000) McGraw-Hill Professional Publishing
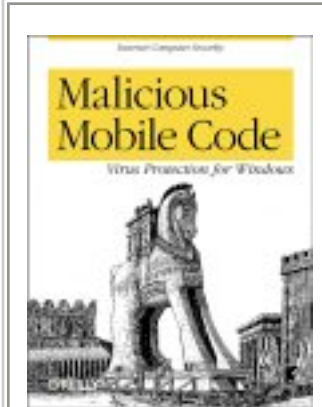
[Malicious Mobile Code: Virus Protection for Windows](#) (O'Reilly Computer Security)
by
Roger A. Grimes
Paperback-542 pages 1 Ed edition (August 2001) O'Reilly & Associates
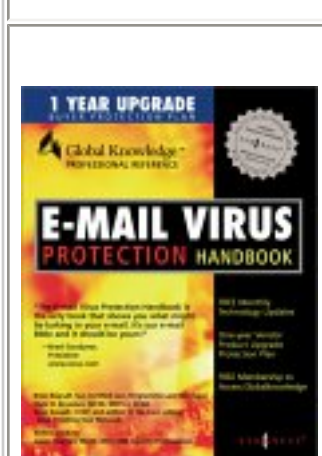
[E-mail Virus Protection Handbook: Protect your E-mail from Viruses, Tojan Horses, and Mobile Code Attacks](#)
by
James Stanger
Paperback-476 pages (October 30, 2000) Syngress Media Inc
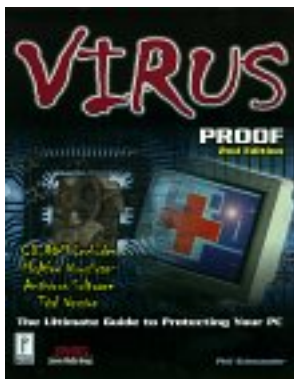
[Virus Proof, 2nd Edition](#)
by
Phil Schmauder
Paperback-350 pages 2nd Bk&cdr edition (July 20, 2000) Premier Press, Inc.

[The Virus Creation Labs : A Journey into the Underground](#)
by
George Smith
Paperback (December 1994) Amer Eagle Pubns
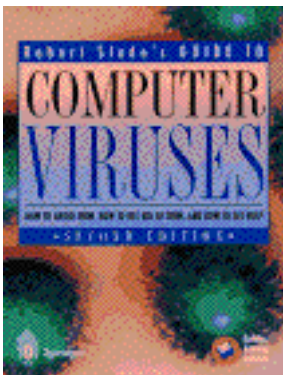
[Robert Slade's Guide to Computer Viruses: How to Avoid Them, How to Get Rid of Them, and How to Get Help](#)
by
Robert Slade
Paperback-422 pages 2nd Bk&Dk edition (June 1996) Springer Verlag

[Computers Under Attack: Intruders, Worms, and Viruses](#)
by
Peter J. Denning (Editor)
Paperback-13 pages (December 1990) Addison-Wesley
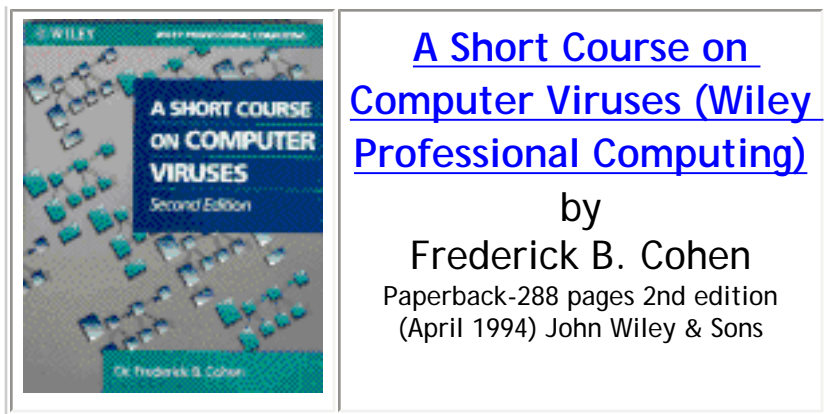
No matter where you get your information, be certain you know the qualifications of the source. Something called the False Authority Syndrome often applies when it comes to virus information.

Summary

- Anti-virus vendor sites are a good source of continuing information.
- Follow discussions on the newsgroups with great care.
- Know the qualifications of sources from which you get information.

Finally, if interested, see some threat details…

Please visit our sponsors.

Click Here to Visit our Sponsor

Protection Intro | Scanning | Integrity Checking | Interception | AV Product Use | File Extensions | Safe Hex | Outlook vs. Outlook Express | Scripting | Backup | On-going Virus Info
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small

payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.

Pray the Rosary for peace.

ckNow.com

Virus Tutorial

Back Orifice

Navigation

Current Threats

Tutorial Map

Anti-Virus Software

Back Orifice is a Trojan that provides a backdoor into your computer when active and you are connected to the Internet. The original program came out in August 1998 with an update called BO-2000 later.

The name is a play on Microsoft's Back Office and the program is advertised as a network management program. It is produced by the group Cult of the Dead Cow (cDc). Even though it does what it's advertised to do, the fact that it installs silently, can't be easily detected once run, and potentially allows a remote user to take complete control of your computer without your permission when it is installed has caused the AV companies to call it a Trojan and they have developed detection routines for the program.

BO is distributed as several programs and documentation. The original programs run on Win95/98 only; Bo-2000 also runs on NT. Indications are BO can be attached to other executables in the same style as viruses. When run, BO silently installs itself (you can't even see it in the task list) and, when the computer is connected to a TCP/IP network (e.g., the Internet) it sits in the background and just listens. What it's listening for are commands starting with *!*QWTY? from a remote computer. The commands themselves are encrypted (in the US version; an international version does not use strong encryption). When a command is received BO is capable of many things; some benign, others quite destructive and/or intrusive. A short list includes: computer info, list disk contents, file

manipulation (including updating itself!), compressing & decompressing files, get and send cached passwords, terminate processes, display messages, access the registry, plus store and send keyboard input while users are logging into other services. BO even supports HTTP protocols and emulates a web server so others can access the user's computer using a web browser. If that's not enough, BO can expand its abilities using plug-ins (which, of course, it can be commanded to download to itself).

As evil as I've made Back Orifice sound, it has legitimate uses for network maintenance and even functions in a manner similar, although much more extensively, to various remote control utilities (e.g., Carbon Copy). The main difference is that they make themselves known while BO completely hides itself.

You probably want to know if Back Orifice is on your system so keep your AV software up to date and make certain detection of programs like it is turned on.

Microsoft has released a security bulletin on BO that fairly well dismisses the program. The cDc have released a point-by-point rebuttal of Microsoft's bulletin. For a bit of entertainment, take a look at:

http://www.cultdeadcow.com/tools/bo_msrebuttal.html

BO-2000 even supplies a plug-in that allows a remote user to see what is on your screen and take control of the mouse and keyboard. Since BO was written with a flexible architecture other plug-ins can be written and remotely installed.

I run the Zone Alarm firewall software and, even though I'm on a dial-up connection and am not on the Internet for long periods I often will see a Back Orifice inquiry against my current IP address in the Zone Alarm logs.

You probably don't want this beast running in the background on your computer.

Click Here to Visit our Sponsor

Current Threats | Back Orifice | CIH Spacefiller | Kakworm | Laroux | Love Letter | Melissa | Nimda | Pretty Park | Stages
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Current Threats

Virus Tutorial

Navigation

Current Threats

Tutorial Map

Anti-Virus Software

CIH Spacefiller

This virus is the classic that illustrates the working and danger of a spacefiller virus type.

It was first reported in June 1998 and dubbed Chernobyl by the press. It infects files written in the Portable Executable (Windows 95 executable) format. This format allows blocks of blank space in the executable and this virus exploits that by attempting to install itself into a single block (or multiple blocks if necessary). Only Win95/98 executables are vulnerable to spreading the virus. DOS and Windows 3.1 executables are not the correct format. NT executables can be infected but will no longer work due to their structure.

The virus has some bugs that cause some programs it tries to infect to stop working and the computer to halt.

The original virus was set to trigger on 26 April, the anniversary of the Chernobyl disaster. Variants trigger on 26 June or the 26th of any month.

The beast is nasty in that it allowed to activate it will attempt to overwrite a Flash BIOS (if found) and then goes on to overwrite the hard disk. It's not always effective at overwriting the BIOS since different BIOS types have different routines needed to write to them; but, if it does,

the chip has to be replaced or, at a minimum, rewritten with the correct BIOS information. Either is a major problem for most users.

The virus spreads rapidly once run on a system. It was a very "popular" virus in 1998 but major infections have since been wiped out due to major press coverage and AV software updates. Despite that, CIH continues to show up.

You most certainly want to have current AV software and not let this beast onto your system. It continues to be dangerous.

Please visit our sponsors.

Click Here to Visit our Sponsor

Current Threats | Back Orifice | CIH Spacefiller | Kakworm | Laroux | Love Letter | Melissa | Nimda | Pretty Park | Stages
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

ccnow.com

Virus Tutorial

Kakworm

Navigation

Current Threats

Tutorial Map

Anti-Virus Software

Kakworm (KAK) is a worm. It takes advantage of a security vulnerability in Microsoft's Internet Explorer browser and Outlook Express mail program. A patch for this vulnerability has been published by Microsoft and should be installed (Microsoft Security Bulletin MS99-032). Non-Microsoft browsers and mail programs are not affected.

KAK is transmitted embedded in the HTML signature to a message. Users don't see it there because there is no displayable text (KAK is written in JavaScript).

Users do not need to click on any attachment or perform any action for KAK to activate. All that is necessary is for the user to view an infected message in the mail preview window (or open the mail and view the message).

Once activated, KAK saves the file KAK.HTA into the Windows Startup folder. The next time the computer is started, KAK.HTA runs and creates KAK.HTM in the Windows directory. The registry is changed so that KAK.HTM is included as a signature on all outgoing mails. This activity is controlled by a new \AUTOEXEC.BAT file (the original file is saved to \AE.KAK).

After 5pm on the 1st of any month the worm displays the

message "Kagou-Anti-Kro$oft says not today" and then shuts the computer off.

KAK is based on Bubbleboy, the first worm able to spread without a user having to open an attachment.

Please visit our sponsors.

Click Here to Visit our Sponsor

Current Threats | Back Orifice | CIH Spacefiller | Kakworm | Laroux | Love Letter | Melissa | Nimda | Pretty Park | Stages
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Virus Tutorial

Navigation

Current Threats

Tutorial Map

Anti-Virus Software

Laroux

Sneaking up on the world in July 1996 while everyone was so worried about Word macro viruses, Laroux became the first Microsoft Excel macro virus and opened up yet another data file to worry about.

Laroux is a fairly simple macro virus. The original contains two macros: AUTO_OPEN and CHECK_FILES. The first tells Excel to run the second as soon as a worksheet is opened. CHECK_FILES will look in the Excel startup path (usually the XLSTART directory) for a file called PERSONAL.XLS. If not found one is created; if found the module LAROUX is created in it. Since PERSONAL.XLS is automatically opend whenever Excel is run (much like NORMAL.DOT under Word) the virus will be loaded every time Excel is started and all accessed worksheets infected.

Laroux is written in Visual Basic for Applications (VBA), a macro language based on the Visual Basic programming language. Laroux is not intentionally destructive; it just replicates. Variants, however, frequently appear and there is no guarantee they will be benign.

Laroux, in its many variants, is fairly widespread.

Please visit our sponsors.

Current Threats | Back Orifice | CIH Spacefiller | Kakworm | Laroux | Love Letter | Melissa | Nimda | Pretty Park | Stages
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Virus Tutorial

Navigation

Current Threats

Tutorial Map

Anti-Virus Software

Love Letter

A Visual Basic Script worm that spread widely around the world simply because people were too curious for their own good and opened an E-mail attachment without knowing what was in it.

In its original form the worm sent itself to users via an E-mail attachment. The message subject was "ILOVEYOU" and the message text was: "kindly check the attached LOVELETTER coming from me." The attachment was called LOVE-LETTER-FOR-YOU.TXT.vbs (note the double extension). When clicked on the attachment would run (assuming Windows Scripting Host is installed) and the cycle would start again.

The double extension is important for this worm as it tries to exploit an ease of use function. Mail programs and directory programs are often set, by default, to not show extensions. This is supposed to shield you from the details of the computer's operation. In this case, it made things worse since, if you had that option set, the attachment would show up as LOVE-LETTER-FOR-YOU.TXT and thus appear to be a text file instead of an executable script. If you don't see extensions now, reset your options to show them.

In operation, the worm performs several actions:

- It drops an HTM file which is capable of spreading the virus along with an associated mIRC script that tries to use the HTM file.
- It checks for the file WinFAT32.exe in the IE download directory. If not found the worm changes the registry IE startup page to one of a few websites where the file WIN-BUGSFIX.exe will be downloaded and set to run on the next computer start.
- The IE start page is set to blank.
- The worm copies itself into two places where it will be executed on each computer restart.
- It will try to send itself to every entry in your Outlook address book.
- The worm searches all drives (local and networked) for files ending in VBS, VBE, JS, JSE, CSS, WSH, SCT or HTA. If found, they are overwritten with the virus and their extension renamed to .VBS.
- Graphics file with JPG or JPEG extensions are also overwritten with the virus and .VBS added to their name (so they will end up with a double extension).
- Multimedia files with MP2 and MP3 extensions are marked as hidden and then copied to a new file with the same name and .VBS added. (Note that of all the files attacked, these are the only ones that can be recovered directly; all others have to be recovered from backups.)
- As mentioned, the worm looks for an mIRC client and, if found, will drop a script and HTM file designed to send the worm over mIRC chat.

The "script kiddies" had a field day with this beast and many, many variants were quickly developed and spread. More than 20 variants have been reported and, over time, you can bet there will be more. A few of the most enticing might be:

Subject fwd: Joke, no body, Attachment: Very funy.vbs

Subject: Mothers Day Order Confirmation, Body: We have proceeded to charge your credit card for the amount of $326.92 for the mothers day diamond special. We have attached a detailed invoice to this email. Please print out the attachment and keep it in a safe place.Thanks Again and Have a Happy Mothers Day! mothersday@subdimension.com , Attachment: mothersday.vbs.

From: support@symantec.com, Subject: Virus ALERT!!!, Body: Dear Symantec customer, Symantec's AntiVirus Research Center began receiving reports regarding VBS.LoveLetter.A virus early morning on May 4, 2000 GMT. This worm appears to originate from Asia Pacific region. Distribution of the virus is widespread and hundreds of thousands of machines are reported infected. etc., Attachment: protect.vbs.

Subject: How to protect yourself from the ILOVEYOU bug!, Body: Here's the easy way to fix the love virus., Attachment: Virus-Protection-Instructions.vbs.

And, many more…

Do not blindly open any attachments to E-mail unless you know exactly what is in them!

Please visit our sponsors.

Click Here to Visit our Sponsor

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Virus Tutorial

Navigation

Current Threats

Tutorial Map

Anti-Virus Software

Melissa

Melissa is a combination Word macro virus and E-mail worm. It was first found on Friday, 26 March 1999 and spread very rapidly around the world.

Basically, when a user clicked on the DOC file attached to the E-mail they would run the included Word macro virus. One of the first things the virus would do is to format and send a message to the first 50 addresses in your Outlook address book. The subject would be "Important Message From <your username>" and the message body would say "Here is that document you asked for …don't show anyone else ;-)". Attached to this message is the current document you are working on. Since Melissa is a virus and infects the Word NORMAL.DOC file it's possible that the infected file sent out could be something very important from your system and not just the infected document you received.

In the rare case where the minute and day of the month are the same (e.g., 8:08 on 8 July) the virus will insert the phrase "twenty-two, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here." into the current document. (This is a reference from the Simpsons cartoon series.)

The initial distribution of Melissa was as a file called

LIST.DOC that contained passwords for X-rated websites. It was posted into the usenet group alt.sex.

There are a significant number of Melissa variants.

Please visit our sponsors.

[Click Here to Visit our Sponsor]

Current Threats | Back Orifice | CIH Spacefiller | Kakworm | Laroux | Love Letter | Melissa | Nimda | Pretty Park | Stages
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Current Threats

Virus Tutorial

Please visit our sponsors.

Nimda

Nimda is one of the more complex virus/worm constructs released. It infects files, spreads itself via E-mail, spreads via Web sites, and spreads via local area network exploits. It infects all versions of Windows from Win95 through Win2000 as well as Microsoft's IIS.

Navigation

Current Threats

Nimda is credited with several "firsts" in its infection techniques. It is the first beast to infect .EXE files by embedding them into itself as a resource. It also infects Web pages so unsecured browsers will infect upon viewing the Web page. Finally, Nimda is the first worm to use any user's computer to scan a network for vulnerable machines behind a firewall to attack (in the past only infected servers did that).

Tutorial Map

Anti-Virus Software

Nimda uses several known weaknesses in Microsoft IIS servers. It would not have spread as far as it did had administrators applied the known patches. For reference, the patches are at…

- Unicode exploit:
  http://www.microsoft.com/technet/security/bulletin/ms00-078.asp
- MIME exploit:
  http://www.microsoft.com/technet/security/bulletin/ms01-020.asp

Nimda uses these methods to spread:

- from client to client via E-mail and an infected .EXE file
- from client to client via open network shares
- from web server to client via browsing of compromised Web sites
- from client to Web server via active scanning for and exploitation of the "Microsoft IIS 4.0 / 5.0 directory traversal" vulnerability

- from client to Web server via scanning for the back doors left behind by the "Code Red II" and "sadmind/IIS" worms.

File Infection. In one mode, Nimda acts like any standard file infector with a new twist. It searches for .EXE files and adds them to itself as a resource. When the .EXE file is on a server downloads then spread the beast. Additionally, if the file is on a local computer, sharing that file can also spread the beast.

When an infected file is run the worm extracts the original program and runs it. Nimda attempts to delete this file after it finishes but cannot always do this. In that instance it creates WININIT.INI with commands to delete the file the next time Windows starts.

Nimda finds .EXE files to infect by searching the keys [SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths], [Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders], and all subkeys. Strangely, WINZIP32.EXE is not infected.

E-mail Worm. In another mode, Nimda acts like any other worm. It searches your E-mail client address book(s) and HTML files on your computer for E-mail addresses and then sends itself to these addresses in an attached file. An E-mail from the worm comes as a "multipart/alternative" message with two sections. The first is defined as MIME type "text/html", but contains no text (the message appears empty). The second is defined as MIME type "audio/x-wav", but contains a base64-encoded attachment named README.EXE, which is a program.

Many users can be tricked into opening such attachments and any mail software running on Windows that uses Microsoft Internet Explorer 5.5 SP1 or earlier (except IE 5.01 SP2) to render the HTML mail **automatically** runs the attachment and infects the machine. (both bad practices!).

Nimda uses its own SMTP server to send E-mail messages.

Web Worm. Using one of the known exploits listed above, Nimda scans the Internet for Microsoft IIS Web servers. When a server is found, if it has open security holes, Nimda enters and modifies random Web pages on the server (as well as .EXE files found on the server). The modifications allow the worm to spread to users simply browsing the infected site.

To do this, Nimda searches drives for .HTML, .ASP, and .HTM files. When found, it adds a small JavaScript snippet to the end of the files. This code opens a file named README.EML when loaded by a Web browser.

README.EML is another form of the worm (MIME-encoded) deposited into directories where the .HTML file were found. Browsers not patched (see MIME exploit above) will automatically execute this file with no user input. Users will not see the worm running as it runs in a minimized window.

File Share Propagation. Infected computers on a local network will search for other computers with open file shares. When found, Nimda will transfer a hidden/system file (RICHED20.DLL) onto the other computer in any directory where .DOC or .EML files are found. After that, if any of these files are opened in Word, Wordpad, or Outlook the hidden RICHED20.DLL file will also be automatically executed. This will infect the that computer.

Additionally, Nimda will try to replace the Windows RICHED20.DLL master file and will place .EML (and sometimes .NWS) files into folders it accesses.

Nimda On Your Computer

Nimda usually shows up as a README.EXE attachment to an E-mail, but can show up as any .EXE file with over five characters in the rootname. If run, it first copies itself to a temporary directory with a random name of the form MEP*.TMP (where * represents random characters). It then runs itself from that folder using the command line option "-dontrunold").

The first thing the launcher does when running is to see if it has enough resources to run the main worm. If so, it extracts itself from the infected .EXE file and executes. Using the current time and some arithmetic operations the worm determines if it can delete files from the temporary folder. Once that is done, the worm builds it's primary infection tool: a MIME-encoded copy of itself and multi-part message that can be attached to. This latter is given a random name and stored in a temporary directory. Now it's ready to get to work.

Nimda next looks for the process called "Explorer." In some cases it opens this process and assigns itself to a remote thread under Explorer. If that fails the worm uses API information to get needed information about the local computer. Then, it rests.

When it wakes up Nimda checks to see what operating system it's running on. If NT-based, it compacts itself and copies itself out to LOAD.EXE in the Windows\System folder. The SYSTEM.INI file is then modified to start with the shell EXPLORER.EXE (as usual) but with "LOAD.EXE - dontrunold" as

well. This assures the worm will run at each system start.

Finally, the worm copies itself to RICHED20.DLL, also in the System folder, and sets the file to hidden and system. When that's done Nimda looks for shared network resources and starts to scan files on remote computers. Here it's looking for .DOC and .EML files and, when found, RICHED20.DLL is copied to their directory so it will be run when an OLE component is needed on the remote computer. This, then starts the infection process on the remote computer.

While looking around the remote computer Nimda also copies infected .EML and (sometimes) .NWS files with names similar to HTML files already found on that remote computer. These files can also infect the remote computer if accessed.

Using the IP address of the infected computer, the worm searches for IIS servers to infect using a known backdoor (a patch is available, see the notes at the start of this page). The idea is that if the current computer is not properly protected then other local computers may not be as well so 50% of the probes (approximately) will be using near-by IP addresses.

Some other things the worm does…

- It modifies the key [Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced] so that hidden files are no longer seen. This hides the worm in Explorer.
- It adds the account "guest" to an infected system and gives it Administrator and Guests group priviledges. Using this it shares the C:\ drive with full access priviledges.
- It deletes subkeys from the key [SYSTEM\CurrentControlSet\Services\lanmanserver\Shares\Security] which effectively disables sharing security.

This beast places itself in a number of different locations so it is easy to overlook one or more if you're trying to disinfect manually. It's best to use a tool to do any disinfection. Many Anti-Virus sites have free tools to help with this job. Use them.

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.

Copyright © 2001 Computer Knowledge, All Rights Reserved
[Pray the Rosary](#) for peace.

cknow.com

Current Threats

Virus Tutorial

Navigation

Current Threats

Tutorial Map

Anti-Virus Software

Pretty Park

This is a combination beast: a worm, a password-stealing Trojan, and a backdoor. June 1999 it was active across Europe and another outbreak was noted March 2000. There are a number of variants.

As a worm, the beast attaches itself to E-mail messages as the file PRETTY PARK.EXE. The associated icon shows a character from the cartoon show South Park.

When first run, the worm looks for an active copy in memory. If not found, it registers itself as a hidden application (i.e., it won't show up in the Windows Task List) and runs its install routine. This routine copies the worm to your Windows System directory as the file FILES32.VXD and then modifies the registry so that this file runs when any EXE file executes. (If you just delete FILES32.VXD and don't fix the registry then EXE files won't run any longer.)

If an error occurs during install the worm tries to run the 3D Pipes screen saver (SSPIPES.SCR) and, if not found, the CANALISATION3D.SCR screen saver.

Continuing, the worm next opens an Internet connection and runs two routines; one every 30 seconds and the other every 30 minutes. The first attempts to make an IRC chat connection to one of 13 servers. An attempted message is sent and via this the worm author could monitor which computers are now infected. The IRC server list includes:

irc.twiny.net
irc.stealth.net
irc.grolier.net
irc.club-internet.fr
ircnet.irc.aol.com
irc.emn.fr
irc.anet.com
irc.insat.com
irc.ncal.verio.net
irc.cifnet.com
irc.skybel.net
irc.eurecom.fr
irc.easynet.co.uk

As a backdoor, the worm can be used as a complete remote access tool. System information can be sent out, directories created/removed, files sent/deleted and executed. In short, if you can do it, the worm author can also.

The 30-minute routine accesses your Outlook address book and sends messages with the worm attached to those in your address book. The Subject is "C:\CoolProgs\Pretty Park.exe" and the EXE worm file is attached. Anyone running the attachment gets infected.

Overall, a nasty beast; best left alone!

Please visit our sponsors.

Click Here to Visit our Sponsor

Current Threats | Back Orifice | CIH Spacefiller | Kakworm | Laroux | Love Letter | Melissa | Nimda | Pretty Park | Stages
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

ckmow.com

Current Threats

Virus Tutorial

Navigation

Current Threats

Tutorial Map

Anti-Virus Software

Stages

An E-mail worm believed to be the first to use the scrap file format to spread. Before going further, let's first look at what a scrap file is…

Scrap Files.

A scrap file is a type of file used to transfer objects between programs on Windows computers. A scrap file can contain just about anything from simple data, to a document or spreadsheet, to an executable program.

The scrap file can be named with most any extension to make it look like a benign file (e.g., .GIF, .JPG, .TXT, etc.) and then Windows adds the .SHS extension to that. In most cases, even if you have Windows set to show all file extensions, the .SHS extension will not show up after you've saved the file to disk (it should be visible as an attachment to an E-mail message). This can make scrap files more dangerous as they can easily appear to be something they are not just by giving the file a benign name.

Windows assigns "RUNDLL32.EXE SHSCRAP.DLL, OPENSCRAP_RUNDLL %1" to the .SHS extension by default and, when opened, Windows will unpack the scrap file and open or execute whatever is in the file. You will have no control over this once you attempt to open the scrap file.

There is really never any reason for anyone to send you a scrap file. If you ever receive one via E-mail you should delete it without attempting to open it. Tell the sender to send you the actual object instead if you think there was something useful involved. The main reason is that scrap files can easily hide code without any indication of what that code really represents so there is no guarantee the scrap file will be what you think it is.

Advanced note: The display of the .SHS extension is controlled by the following registry entry…

HKEY_CLASSES_ROOT\ShellScrap

"NeverShowExt"=""

If you want to experiment **[Computer Knowledge takes no responsibility if you do!]** you can either change "NeverShowExt" to "AlwaysShowExt" or simply delete the entry. Then, reboot and .SHS files should show their extension even when saved to disk.

VBS/Stages Worm

This is an E-mail worm that spreads via Outlook and mIRC or Pirch IRC chat.

E-mail copies are sent (once only) via the Outlook address book and subjects are constructed from the following list of terms: "Fw:", "Life Stages", "Funny", "Jokes", and " text".

The message itself may contain "The male and female stages of life." The attachment (the worm itself) is in a file named LIFE_STAGES.TXT.SHS (again, like many before it, note the double extension; you should be able to see it in your E-mail program but not after saving the file to disk--see discussion above).

This is the first worm known to use the scrap file (SHS) file type to send its code. When run, the worm creates and displays the file LIFE_STAGES.TXT containing humourous text about stages of life (the text is below).

The male states of life:	
Age.	**Seduction lines.**
17	My parents are away for the weekend.
25	My girlfriend is away for the weekend.
35	My fiancée is away for the weekend.
48	My wife is away for the weekend.
66	My second wife is dead.
Age.	**Favorite sport.**
17	Sex.
25	Sex.
35	Sex.
48	Sex.
66	Napping.

Age.	Definition of a successful date.
17	Tongue.
25	Breakfast.
35	She didn't set back my therapy.
48	I didn't have to meet her kids.
66	Got home alive.

The female stages of life:

Age.	Favorite fantasy.
17	Tall, dark and handsome.
25	Tall, dark and handsome with money.
35	Tall, dark and handsome with money and a brain.
48	A man with hair.
66	A man.

Age.	Ideal date.
17	He offers to pay.
25	He pays.
35	He cooks breakfast next morning.
48	He cooks breakfast next morning for the kids.
66	He can chew his breakfast.

The worm then creates the file SCANREG.VBS with its code and sets the registry so SCANREG.VBS runs at each startup.

It also moves the program REGEDIT.EXE to the recycled directory and changes its name to RECYCLED.VXD (this is an attempt to keep you from editing the registry to remove the worm).

The default icon for .SHS files will also be reset to the default icon for text files and .SHS not shown.

Expect many variants of this type of attack; probably with payloads.

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
[Pray the Rosary](#) for peace.

ck**now**.com

Virus Plural: Viruses

Virus Tutorial

Navigation

Misc. Terms

Tutorial Map

Anti-Virus Software

The correct English plural of **virus** is **viruses**. Please consult any good dictionary before making up words.

For the purists, *in Latin*, there is a rarely-used plural form:

virus, viri (neuter)

(Forms: almost always restricted to nominative and accusative singular; generally singular in Lucretius, ablative singular in Lucretius)

The point of this is that even in Latin the form "viri" is rarely used. The singular form is used in most every instance. (This is from the Oxford Latin Dictionary.)

So, when considering the Latin: "virii" is incorrect and "viri" was almost never used.

Despite the fact there was little use for the plural form, there is another reason why "viri" was rarely used. The most common Latin word for "man" is "vir" with "viri" being its plural in the form used as the subject of a sentence. Thus, since "men" as the subject of a sentence would be used far more often than "venoms" (virus means venom) the "viri" word was most commonly seen as the plural of "man."

Bottom line: Don't try to make up words using a false Latin

plural form. Since the word virus in its English form is now used then the English plural (viruses) should be used.

Please visit our sponsors.

Click Here to Visit our Sponsor

AV Software | License | Virus Plural | Partition Sector | DOS Boot Sector | FDISK /MBR | False Authority | Logic Bombs | Trojans |
Worms
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

cknow.com

Partition Sector

Virus Tutorial

Navigation

Misc. Terms

Tutorial Map

Anti-Virus Software

On hard (fixed) disk drives, the very first sector is the partition sector (often known as the Master Boot Record [MBR] or partition table). Each physical hard disk drive has one of these sectors.

A single physical disk can be partitioned into one or more logical disks. For example, you may have a physical drive partitioned into C: and D: logical disks so that your single physical disk appears (to DOS/Windows) to be two logical disks. The single partition sector contains the information that describes both logical disks. If the partition sector is damaged, then DOS/Windows may not even recognize that your disk exists.

The partition sector also contains a program that is executed every time you power up or boot your PC. The program part of the partition sector is often called the Master Boot Record (MBR) and this term is often used to include both the program half and data half of the sector. The MBR executes and reads the DOS boot sector that also contains a program. Many viruses plant their code in the MBR. Some of these leave the partition data alone; some hide it in another location on the disk; some even move and encrypt that information.

Note: It's important to use a good anti-virus program to fix any MBR infections. Because some viruses move and encrypt the partition information, if you remove them from the MBR

using generic DOS techniques (e.g., the [DOS FDISK program](#) with an undocumented parameter) you can cause more problems than you had with the virus.

Please visit our sponsors.

[Click Here to Visit our Sponsor](#)

[AV Software](#) | [License](#) | [Virus Plural](#) | [Partition Sector](#) | [DOS Boot Sector](#) | [FDISK /MBR](#) | [False Authority](#) | [Logic Bombs](#) | [Trojans](#) | [Worms](#)

[Virus Tutorial Home](#) | [Virus Intro](#) | [Virus Types](#) | [Virus History](#) | [Virus Protection](#) | [Virus Hoaxes](#) | [Current Threats](#)

[Home](#) | [Products](#) | [Definitions](#) | [Newsletter](#) | [Virus Tutorial](#) | [Contact](#)

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

DOS Boot Sector

** cknow.com**

Virus Tutorial

Navigation

Misc. Terms

Tutorial Map

Anti-Virus Software

When a floppy diskette is formatted (it doesn't matter if it's a system or data disk) the very first portion of the disk is set aside for two main purposes:

- storing information about the disk, and
- storing a short program that either puts a message on the screen saying the disk cannot be used to start the computer if it's a data disk, or a short program that starts to load the operating system if it's a system disk which can start the computer (boot disk).

This special sector is numbered 0,0 and is called the Boot Sector.

A hard disk also has a DOS boot sector, but it's located in a different sector on the hard disk (see note at the end of this article). Other removable devices have DOS boot sectors that are defined by the format utility for that device. Bootable CD-ROMs, if infected by whomever wrote out the disc, could also be the source of an infection.

Since the DOS boot sector is executed every time you power on or boot your PC, it is very vulnerable to virus attack. Damage to this sector can make your disk appear to be unreadable. This sector is rewritten whenever you do a "SYS" or a "FORMAT /S" to a disk.

Warning: Even a non-bootable floppy can contain a virus

in the boot sector. If you leave an infected floppy in your PC when you power on or boot, you will be infected even though the PC won't successfully boot from that floppy.

When a hard disk is formatted (FORMAT command) a boot sector, similar to that on a floppy diskette, is also created. **Note:** This boot sector should not be confused with the [Master Boot Record](#) (MBR) on a hard disk. In order to distinguish between the two, we've adopted the terminology of DOS Boot Sector (DBS) for the boot sector created by FORMAT on a hard disk.

[AV Software](#) | [License](#) | [Virus Plural](#) | [Partition Sector](#) | [DOS Boot Sector](#) | [FDISK /MBR](#) | [False Authority](#) | [Logic Bombs](#) | [Trojans](#) | [Worms](#)

[Virus Tutorial Home](#) | [Virus Intro](#) | [Virus Types](#) | [Virus History](#) | [Virus Protection](#) | [Virus Hoaxes](#) | [Current Threats](#)
[Home](#) | [Products](#) | [Definitions](#) | [Newsletter](#) | [Virus Tutorial](#) | [Contact](#)

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

cknow.com

FDISK /MBR Problems

Virus Tutorial

FDISK /MBR is often suggested as a solution for fixing a virus attack.

The simple advice is: Just Don't Do It!

Navigation

Misc. Terms

Tutorial Map

Anti-Virus Software

One "cure" for partition sector viruses suggested by people who think they know what they are doing is the FDISK command using the undocumented parameter /MBR. But, understand that there are good reasons why the /MBR parameter is **undocumented**. **It is dangerous.**

The following [somewhat edited] detailed description was posted to comp.virus by Nick FitzGerald and is used with permission.

<Start quote>

Before describing what can to wrong, let's first see what the command does…

To understand what it does, first we have to get some terminology clear. The Master Boot Record (MBR) of a PC's hard drive is the very first physical sector on the disk (0,0,1 in head, cylinder, sector terms). There are some special things about the MBR. It contains (at a minimum) some

executable code to start the bootstrap of the operating system, a 64 byte data area known as the partition table and a two byte signature (that some BIOSes reputedly do not check for).

Assuming that the basic BIOS hardware integrity tests pass and the BIOS configuration is set to allow booting from a hard drive, at power-up the MBR will be copied from the disk and execution passes to the beginning of the MBR. Standard DOS MBRs (they have slightly different code for different DOS versions and other operating systems) then analyze the partition table to find a primary, active DOS partition, and, if found, (there are other conditions depending on the DOS version among other things) the first sector of that logical partition (the operating system boot sector) is loaded into memory and execution passes to it (and that traditionally bootstraps the operating system proper). This may seem to be getting away from the MBR, but you also need to understand something about the typical disk layout of these structures.

Since DOS 3.0 the DOS boot sector has conventionally started at the first sector of a track (often 1,0,1, but never count on it). This has meant that all of the first physical track except the MBR (first sector) is "wasted space."

Now, on to what FDISK/MBR does…

Normally it overwrites what would be the DOS pre-bootstrap code part of the MBR, leaving the partition table and signature mentioned earlier.

Generally though, it sounds fairly harmless, right? "Generally" it is, and that explains why on many, many machines thousands of people have ignorantly done no damage to their drives.

The problem is, there are an awful lot of machines where my earlier description of the MBR contents and the layout of things on the first track of the hard drive do *not* match what

FDISK is programmed to assume, and, as an Information Technology professional, I cannot conscientiously recommend something that can trash someone's disk without giving them a clear understanding of the possibility of making matters worse. This is why I refuse to post submissions that basically just say "Try FDISK/MBR" in response to "How do I clean <some boot virus>?" questions.

Examples of things that can go wrong and what happens:

A security system that does on-the-fly encryption and decryption of the hard drive may be installed with a pre-OS "driver" loading from the MBR bootstrap code. Such a scheme, being non-standard, has its own special MBR bootstrap code. Such code is typically much more than one sector (512 bytes) and as there is no DOS to interpret the file system, the "driver" is usually stored in the "wasted space" on track one (after the MBR) I referred to earlier. (A dual-boot MBR, e.g., OS/2, is another example that might fit into this category.)

You will lose access to your drive, at least until appropriate actions can be taken to reinstall the encryption software. Well-designed software of this kind will have been designed with data-integrity as well as security in mind so should have install options to allow reinstalling over a "corrupted" setup. Once FDISK/MBR has been run, the hard drive will most likely be completely inaccessible (after all, this is the point of most disk encryption schemes). Given someone was ignorant enough to corrupt it in the first place, what do you reckon the chances are they will have any idea

they had a disk encryption scheme in the first place? (Or, at least, what are the chances they know how to have the installation fixed?)

A virus that does not preserve the original partition table in the right place **or** that encrypts it.

How many people do we get here [posted in the newsgroup comp.virus] per year with horror stories of "losing their C: drive" after FDISK/MBR against a Monkey-infected drive (or several other quite common viruses that also do not preserve the MBR in place)? These are usually quite easily fixed once someone who really knows what they are doing gets involved (unless the "expert" who just trashed the disk insists on continuing...).

A pre-OS driver to support "large drives" has been installed so a drive greater than 528MB can be used in a machine with an "old" BIOS. The mechanism for this is much the same as in 1 above.

Such large disk drivers (which are effectively a software BIOS extension) are quite common. (Anyone with a machine more than about 18 months old who has "upgraded" their hard drive is likely running one.) FDISK/MBR removes the driver that correctly allows access to cylinders 1024+, but the effect of removing it varies depending on all kinds of variables to

do with the machines BIOS, the way the drive was partitioned, etc. As with encryption systems, many users of such large disk drivers have no idea that they are running one--after all, computers are just "tools", you don't have to understand how they work to use them. Because the driver load mechanism is similar to the security products mentioned in 1, similar comments apply about fixing these should they be damaged by an unwanted FDISK/MBR.

A virus that leaves the partition table in place, but stores critical viral variables **in** what is normally the bootstrap code portion of the MBR. A particularly nasty possibility here is that a virus may be running on-the-fly encryption/decryption of the drive's contents using an encryption key that was randomly generated at infection time.

At least one family of "in the wild" viruses, One_Half, does what I described here. FDISK/MBR against a drive infected with a One_Half variant (or any future/unknown virus that uses a similar "trick") will remove the MBR infection (One_Half is multi-partite, so it doesn't necessarily clean One_Half completely), *but* leaves you with a hard drive whose contents are partially encrypted with a now unknown *and* irretrievable key. This is definitely a case of the "cure" being worse than the disease!

Some antivirus (or general "system integrity")

software may have loaded a special MBR to allow itself to check for possible MBR infection/change attempts.

FDISK/MBR against such integrity systems has a wide range of effects depending on the design of the system, from simply warning you of a change to the MBR to completely locking you out of your hard drive until the system is reinstalled/reconfigured.

A currently unimplemented virus attack I will not describe in detail here.

I know of a boot virus attack that has only been partially implemented in a real world virus to date, where FDISK/MBR would apparently clean the virus, but on rebooting from the hard drive, the virus would be able to reinstall itself *and* would "know" that a (clumsy) disinfection attempt had been made against it. If the virus' author was so inclined, this could be used as a trigger for some nasty payload (like reformatting your drive).

I could have named examples of the first five, though the risk in doing that is people who do not know better will think they are the **only** possibilities, rule them out and blunder on.

Just in case it is not clear at this point, all of these things *replace* (part of) the "normal" bootstrap code in the MBR with their own code and/or data and in some way critically modify the function of the bootstrap process.

Now you understand why FDISK/MBR is *DANGEROUS*!

<End quote>

Bottom line:

Don't Use FDISK /MBR!

Please visit our sponsors.

Click Here to Visit our Sponsor

AV Software | License | Virus Plural | Partition Sector | DOS Boot Sector | FDISK /MBR | False Authority | Logic Bombs | Trojans |
Worms
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

ckmow.com

Virus Tutorial

Navigation

Misc. Terms

Tutorial Map

Anti-Virus Software

False Authority Syndrome

by
Rob Rosenberger

The information in this section was provided by and used with permission of Rob Rosenberger who can be reached on the web at:

http://www.vmyths.com/

True story. A couple of years ago I dropped by the Software Etc. store in Fairview Heights, Illinois just to browse. Another customer had come in before me and told an employee about a problem with his video monitor. The employee warned the customer he had contracted a newly discovered computer virus, which he proceeded to describe in great detail.

I interrupted the employee. "Sir, you have it completely wrong. That virus doesn't exist. It's the latest hoax."

"Oh, no," the employee replied. "We've got E-mail reports from our sales headquarters telling us to keep our eyes open for it."

To which I countered, "Some upper-tier sales manager has

been duped and is telling you BS. McAfee Associates and others have issued public statements dismissing that virus as a hoax. What you've described simply cannot be done by any virus. Period."

I then turned my attention to the customer. "Stop listening to this guy. You don't have this magical virus he's describing because it simply doesn't exist. You have some other problem with your video monitor."

What credentials did this salesman hold in the field of computer viruses? He may have flipped hamburgers at a McDonald's restaurant two weeks earlier for all we know. Right now he sells merchandise at a computer store--does this qualify him to give advice about computer viruses?

Most people who claim to speak with authority about computer viruses have *little or no* genuine expertise. Some virus experts describe it as "False Authority Syndrome"--the person feels competent to discuss viruses because of his job title, or because of his expertise in another computer field, or simply because he knows how to use a computer.

I want you to question the credentials of anybody who talks about computer viruses.

The U.S. Air Force highlights the concept of False Authority Syndrome in *Tongue & Quill*, their official publication on effective writing:

> *Nonexpert opinion* or assumed authority--Don't be swayed (or try to sway someone else) based on the opinion of an unqualified authority. The Air Force is chock-full of people who, because of their *position* or authority in *one* field, are quoted on subjects in other fields for which they have limited or no experience."

In a word…

> **ultracrepidarian:** (n., adj.) a person who gives opinions beyond his scope of knowledge.

(As this Air Force publication notes, False Authority Syndrome can attack people in *all* fields of expertise.)

Computer salesmen, consultants, repairmen, and college computer teachers often succumb to False Authority Syndrome. In many cases a person's job title sounds impressive, but his or her job description at most may only include references to vague "computer security" duties.

Network administrators typically fall into this category. Most hold the title of "company virus expert" simply because their job description includes network security. They may have no real education in computer security, but their experience in the field of computer networking gives them confidence when talking about the *unrelated* field of computer viruses.

People who suffer from False Authority Syndrome too often assert conclusions from insufficient data and they habitually label their assumptions as fact. Quoting again from *Tongue & Quill*:

> "We jump to conclusions from too little evidence; we rely too much on 'samples of one' (our own experience); something happens twice the same way and we assume the ability to *forecast*… Unfortunately, our natural desire is to make positive, solid statements, and this desire encourages the asserted conclusion."

Consider the case of Gary L. Allen. Writing in a letter to *Computerworld*, he offered his analysis of 1992's worldwide Michelangelo virus scare. Allen listed his virus-fighting credentials: "I am an MIS manager, and we found Michelangelo on disks distributed by one of our software

vendors, and it never made it into our local-area network."

Allen went on to say: "If we had not been prompted [by the media] to scan [for the Michelangelo virus]… it surely would have made it onto the network hard drives and from there who knows where."

Allen made "positive, solid statements" as *Tongue & Quill* notes. Amazingly, this network administrator claims he checked for a virus because the *press* told him to do so! Allen also assumes the Michelangelo virus "surely would have" infected his network drives. Virus experts could easily debate this, but why must they debate him in the first place? Allen's own words expose him as a virus pseudo-expert.

Virus Pseudo-experts

I once lectured about viruses to a small group of businessmen in 1991. A network administrator stood up at one point and proclaimed his company (a law firm) would literally *close its doors for good* "if a destructive virus of any type gets on our system." They would sell the office equipment; the secretaries would find new jobs; the lawyers would take their filing cabinets to other firms. The company would fold if even *one* destructive virus infiltrated their network.

Shocked by his statement (and trying to regain control of the lecture), I asked what would happen if fire swept through the firm's building. No sweat: they kept backups off-site and had purchased contingency contracts for just such emergencies. I responded, "Well, there you go. If a virus ever gets on your computers, burn your building to the ground and your problem is solved!"

The audience laughed--but I fumed. I would *fire* this man on the spot if he worked for my company! I don't want anyone on my payroll who would instantly put everyone out of work due to his own pompous ignorance.

Sadly, ignorant network administrators all too often perpetuate myths about the dangers posed by computer viruses. Ken Hall, a manager at Georgia Tech's Financial Data Technology Office, wrote a typical story for *Atlanta Computer Currents* magazine in response to the Michelangelo scare of 1992. Hall's seventh paragraph touts a common myth: "Traditionally, viruses have infected computers that have downloaded programs form *[sic]* dial-up bulletin boards." Experts have worked for years to squelch this myth and others, but pseudo-experts like Hall greatly outnumber them.

Computer Security Experts

Some people hold a rare position in large companies where their entire job title *is* "computer security." It's not just an additional duty. Their job covers the whole range of security issues, from teenage hacking to espionage, from fires to natural disasters--and of course computer viruses. You'll find False Authority Syndrome here as well.

Computer security personnel at Scott Air Force Base, Illinois attended a job-related course in early 1995. The course included a special handout: Russell & Gangemi's *Computer Security Basics*, a book last updated in 1992. Computer books typically have short lifespans: many will disappear from store shelves within a year. But *Computer Security Basics* serves as an industry reference and you could still find it at Waldenbooks stores in mid-1996.

Russell & Gangemi mention the shareware program "Flu_Shot" by name on page 88 and tell readers they can obtain it "from both commercial and public domain sources," i.e., from BBSs. Yet on page 87 the book warns readers to "be wary about new public-domain or shareware programs… Don't allow users to install software obtained from [BBSs]."

This contradiction sounds minor on the surface; in reality it perpetuates a common virus myth. Specifically, it helps fuel

a myth among *computer security personnel*. Russell & Gangemi also recommend readers to the "Computer Virus Industry Association," an organization widely dismissed *before the book's first publication* as a publicity front for antivirus mogul John McAfee.

Computer security personnel don't just read books--they watch training videos, too. ViaGrafix, a company specializing in computer training videos, markets a video about computer viruses. Produced in 1992 and still sold as of June 1996, the ViaGrafix video touts the mythical story of the "Gulf War virus." Again, this only helps fuel myths among computer security personnel.

Wolfgang Stiller, an internationally recognized virus expert and author of the "Integrity Master" antivirus program, says "computer security experts today--people who *deserve* that title--tend to have a good background on how viruses operate. They can dispense some good advice." But he chooses his words carefully when asked to comment on virus *expertise* among computer security personnel.

"They're a little more likely than the average person to understand viruses," Stiller notes. "Some would say they're a *lot* more likely to understand them, but I've met a fair number who don't know a thing about viruses, or, even worse, they've got misconceptions. In light of the fact they are computer security experts, their misconceptions carry a lot more weight than the average person. Errors are much more damaging when they come out of the mouths of these people."

Stiller sums up False Authority Syndrome among computer security experts: "Put me on a panel with a computer security person, and I won't claim to have his level of security expertise. But the computer security guy will invariably claim to have *my* level of virus expertise. How can you convince the audience in a diplomatic way that he *doesn't*?"

(Stiller offers an interesting analogy: he wonders about the policemen who vouch on TV for The Club®. Do the officers specialize in car-theft investigations--or do they write traffic tickets?)

Computer Repairmen

Network administrators and computer security personnel may hold some of the best job titles, but they don't have a lock on the market when it comes to virus pseudo-experts. The list also includes computer consultants & repairmen. In one example, CompuServe user Rob Parker posted a message in early 1995 lamenting his laptop's dead hard disk:

> "Thinking the problem was a virus, the tech[nician] tried a number of virus scanners, all negative. He then tried to reformat the hard disk… He claimed that the [hard disk] was ruined, and that a virus had done it."

In a nutshell, the repairman used two or more programs to detect viruses on the laptop. None of these programs found a virus. The repairman then tried to reformat the laptop hard disk--but the attempt failed. So he claimed a virus *physically destroyed* Parker's hard disk.

Genuine experts on CompuServe dismissed the repairman's conclusion. Parker now wonders if the repairman made up the story. Did he feel compelled to give his customer an important-sounding excuse for why the drive failed?

Parker got off easy: his hard disk failed during the laptop's warranty period. But his experience raises important questions. How many repairmen incorrectly told customers to fork over money because they claimed "a virus physically destroyed the computer"? How many computer users *believed* it?

Magazines, Newspapers, TV

Paul Mayer, an expert on marketing for small software companies, wrote a regular column for a computer magazine. His editors once paid him to write an article on viruses. Mayer's virus credentials appeared in the fourth paragraph:

> "I have personally had two contacts with viruses in 15 years of working with computers. The first encounter caught me completely off-guard. I was prepared for the second."

Mayer wrote the story from the perspective of a regular user. He believes the magazine picked him to write it *because* of his first-hand user experience with viruses. And to his credit, Mayer consulted with a genuine virus expert while writing the article.

Unfortunately, reporters in the mainstream media will quote almost *anyone* when it comes to viruses--and they habitually quote local people. A typical story illustrates this point. Published in the St. Louis Post-Dispatch during 1992's worldwide Michelangelo virus scare, it quoted various local businessmen, among them:

- Craig Johnson, manager of a local Software Plus store;
- Ernest White, manager of a local Babbage's store;
- Todd Jones, salesman at a local Software Centre store.

This problem afflicts TV reporters as well. An *NBC Nightly News* story at the height of 1992's Michelangelo scare included an interview with a computer salesman. He mentioned his customers' panic and the reporter asked if "the panic is justified." The salesman responded: "yes."

And there you have it: *panic is justified* if you think your computer might have a virus. So says a nationally recognized computer salesman.

Even "computer-literate" mainstream reporters commit

serious blunders when they write stories about viruses. Numerous reporters logged onto CompuServe, GEnie, Prodigy, and America Online during the Michelangelo scare and posted messages to "all." Each message asked the same question: "Want to be interviewed for a story on the Michelangelo virus?"

These reporters didn't search for experts--they went on a "cattle call" for frightened computer users. One *USA Today* reporter, expecting an avalanche of calls, asked people not to tie up his phone unless he or she actually got *hurt* by the Michelangelo virus on its upcoming March 6 trigger date.

Consider the tragic accident where actor Christopher Reeve broke his neck. The mainstream media quickly turned to spinal-injury specialists for comment. Why didn't they ask a *podiatrist* if Reeve will ever walk again?

Podiatrists can diagnose walking disorders and they easily outnumber spinal-injury specialists. But a podiatrist offers the *wrong* expertise in Christopher Reeve's case. The press recognizes this difference. Change the topic to computer viruses--now they'll quote almost anybody with a job in the computer industry.

Never underestimate the mainstream media's role in the spread of False Authority Syndrome. Empirical Research Systems (a computer industry polling firm) conducted a survey in 1991 of corporate employees tasked in some way with computer security. 43% of respondents--almost half--formed their opinions about viruses *just by reading newspapers!*

Newspaper reporters talk to these people to get details (and quotes) for a story. This means the press *feeds* information to virus pseudo-experts, who gladly regurgitate it for other reporters, who write more stories about viruses, which other pseudo-experts read… thus creating an endless circle of misinformation and a never-ending supply of "instant experts."

This same survey concluded with a sad statistic: it estimates *two-thirds* of employees tasked with computer security duties have *inadequate* knowledge about computer viruses.

The "Green Paint Factor"

Interestingly, mainstream reporters sometimes quote computer-industry reporters in stories about viruses. For example, the *St. Louis Post-Dispatch* story mentioned earlier also included a quote from *InfoWorld* editor Ed Foster.

Jeff Duntemann, editor of *Visual Developer* magazine, likens this trend to what he calls the Green Paint Factor. "If you want to extol the virtues of a can of green paint, and the best you can say is that it's *green*--well, it's probably not good paint." If you want to quote somebody about computer viruses, and the best you can say is that he edits a weekly computer publication…

Duntemann continues: "The job of a computer magazine editor [or reporter] is to know a little about a lot in the computer field. He has a considerable *breadth* of knowledge but not a serious *depth* of knowledge, except perhaps in a couple of very narrow specialties."

Why, then, does the mainstream media quote people in the computer press? Duntemann believes computer-industry reporters (and editors in particular) can *speak and write well*. "If you can turn a good phrase about a subject, whether or not you know anything at all about it, then you have a good chance of being labeled an expert," he notes. "Especially by people who know nothing at all about that subject."

John Q. Public

People without impressive job titles suffer from False Authority Syndrome, too. A user who contracts a virus, for example, will often turn around and confidently tell other

people how to avoid them. He or she may even rise to the position of "office virus expert."

False Authority Syndrome plays on two important desires. First, people genuinely like to help others; second, they like to feel in control of their computers. Users easily succumb to the effects of False Authority Syndrome when driven by these natural desires.

"Marcello," a typical user who took a hoax for real, posted a message on CompuServe warning users not to read any messages with "Good Times" in the subject line (lest they contract the so-called Good Times virus). Ironically, Marcello *used* the words "Good Times" in the subject line of his own warning message!

At least one virus expert sent Marcello a playful reply telling him to "stop infecting people" with the Good Times virus. Confronted with details about the hoax, Marcello replied, "Thank you for your help, and I'm sorry, because I was duped, but anyway I was worry *[sic]* about my computer and a lot more from *[sic]* my job."

Implications of False Authority Syndrome

Computer neophytes easily succumb to False Authority Syndrome. They feel more important by spreading the word about dangerous viruses. If someone else points out their errors, these people will often *justify* their actions in terms of fear. As Marcello noted in his apology, he feared both for his computer and for his job.

He probably didn't mean to imply it, but Marcello may believe fear *absolves* his ignorance. After all, if he worried only about his own computer and his own job, then he already *knew* how to avoid the mythical virus: he could feel safe in his own office. But Marcello went a step further by telling others how to avoid the mythical virus.

False Authority Syndrome contributes *significantly* to the

spread of fear & myths about computer viruses. Many pseudo-experts tell users to erect defensive barriers where viruses seldom attack, often leaving typical lines of attack exposed.

Widespread myths & misinformation also convince people to fear *safe* methods of computing and to put their trust in *less-safe* methods. In her book *Rx PC: The Anti-Virus Handbook*, Janet Endrijonas claims "approximately 70 percent of all viruses are boot sector viruses." Wolfgang Stiller and other experts put the total *above 90%.* [This was written before macro viruses and E-mail worms became a significant and growing threat.]

Boot sector viruses, by their nature, don't travel in software downloaded from BBSs--yet pseudo-experts constantly point to downloaded software as the biggest avenue for the spread of viruses.

In his book *Inside the Norton Antivirus™*, Peter Norton dismisses the myth about the dangers of downloaded software. "Bulletin boards do more to spread the awareness of viruses *[emphasis added]*… The primary method of communication concerning viruses is through BBSes *[sic]*." Robert Slade, writing in his book *Guide to Computer Viruses*, goes even further:

> "If I had to choose one viral myth that contributed most to the unchecked spread of [viruses] that exists today, it would be that of the 'safety' of commercial software… The feeling of false security relies on three assumptions: (1) that [software downloaded from BBSs] is a major viral vector, (2) that commercial software is never infected… (3) that there are no viral vectors other than software."

Thanks largely to False Authority Syndrome, users now often panic at the first sign of an odd computer behavior, sometimes inflicting more damage on themselves than any

virus could do on its own (assuming they even had a virus in the first place).

Ross Greenberg earned international fame as one of the pioneers in IBM PC antivirus software. He went into semi-retirement in his mid-30s. Greenberg continues to lecture about viruses, wrapping up with a simple analysis of how he made his fortune: "I'd still be slaving away at a desk for another 25 years if people backed up [their computer data] and kept a cool head."

Conclusion

I don't want to dispel any particular computer virus myths someone may have told you--that's not my goal here. Rather, I want you to *question a person's expertise* if he or she claims to speak with authority on computer viruses. This way we can prevent all the "blind leading the blind" techno-babble. And we can reduce the number of people who believe all the myths out there.

In summary:

- Most people have little or no expertise in the field of computer viruses.
- People with little or no expertise often fall prey to False Authority Syndrome.
- False Authority Syndrome contributes significantly to the spread of fear and myths about computer viruses.
- *Visual Developer* editor Jeff Duntemann sums it up best: "If people exercised greater discretion in who and how and to what degree they place their trust, we would know more as a community--and we would know it better. There would be fewer paths for bad or phony knowledge."

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.

ck now.com

Logic Bombs

Virus Tutorial

Navigation

Misc. Terms

Tutorial Map

Anti-Virus Software

Just like a real bomb, a logic bomb will lie dormant until triggered by some event. The trigger can be a specific date, the number of times executed, a random number, or even a specific event such as deletion of an employee's payroll record.

When the logic bomb is triggered, it will usually do something unpleasant. This can range from changing a random byte of data somewhere on your disk to making the entire disk unreadable. Changing random data may be the most insidious attack since it generally causes substantial damage before anyone notices that something is wrong. It's vital to have software in place that quickly detects such damage.

Although you can detect it after the fact, there is unfortunately no way to prevent a well written logic bomb from damaging your system.

If you've had someone in to do any system work on your computer (e.g., Y2K work) it's particularly important that you independently verify the work was done correctly and to verify no trap doors or logic bombs were inserted into your systems. Work like Y2K modifications require programmers to have detailed access to your systems; just the kind of access someone who wanted to insert a logic bomb into your system would love to have. (This is not to say Y2K contractors are worse than any other person who has low-

level access to your systems; it's just one obvious example.)

Please visit our sponsors.

AV Software | License | Virus Plural | Partition Sector | DOS Boot Sector | FDISK /MBR | False Authority | Logic Bombs | Trojans |
Worms
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

---

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Pray the Rosary for peace.

ckmow.com

Trojans

Virus Tutorial

Navigation

Misc. Terms

Tutorial Map

Anti-Virus Software

These malicious programs are named after the Trojan horse, which delivered soldiers into the city of Troy.

Like the horse, a Trojan program is a delivery vehicle; a program that does something undocumented which the programmer intended, but that the user would not approve of if s/he knew about it. The Trojan program appears to be a useful program of some type, but when a certain event occurs, it does something nasty and often destructive to the system.

Most of the "classic" Trojan programs were delivered to users on disks which advertised themselves as something useful. As an example, a disk that was supposed to contain Aids information was once distributed. Unfortunately, when a program on the disk was run the user's hard disk was encrypted and rendered useless. Many newer Trojan programs make their way to you as E-mail attachments.

There have been many Trojan programs and new ones crop up every day. It's important to know and trust the source of any program you receive because most anti-virus programs can't detect new Trojans. These programs, while potentially destructive, still use common DOS/Windows commands and any attempt to trigger an alert on these commands would result in massive false alarms.

Some anti-virus programs will include Trojans once they are circulating; but by then it may be too late for you.

Two special Trojan threats need to be mentioned for historical perspective:

ANSI Bomb (rare today)

Early text computer applications would sometimes make use of a DOS driver called ANSI.SYS to control display colors and other computer functions. As provided in DOS, ANSI.SYS also has the capability of remapping the keyboard. In order to do this all a user had to do was load ANSI.SYS in the CONFIG.SYS file and then force a particular sequence of characters, starting with the Escape key, to the screen. These would be intercepted by ANSI.SYS and the particular key on the keyboard would then be remapped to perform some defined function.

In the case of an ANSI bomb a Trojan would send a keystroke remapping sequence that might, for example, remap the F1 key to issue a command that might delete everything on the C: drive (or any other unwanted command). The solution, of course, is to not use ANSI.SYS in your CONFIG.SYS file (it's almost never necessary today) and make certain any ANSI simulators you might use as part of a communications program do not implement keyboard remapping.

Windows Help macros (rare but demonstrated)

The Windows Help file format allows various macros to be attached to Windows Help files. These macros can be set to run when the Help file first starts and, right now, there is no way to prevent this from happening. These macros can contain unwanted actions. As of this writing, the only example of this makes changes to your Windows INI files; but, other actions are possible. One researcher has postulated a possible Help file virus, but in looking at what would be necessary to create such a virus (it's not entirely clear it's even possible) Computer Knowledge feels the possibility of one in the wild is remote at best. Anti-virus programs do not generally protect against Windows Help file attacks at the moment so current backups are very important!

Some researchers consider a virus a particular case of a Trojan horse; others believe that if a virus does not do any deliberate damage it cannot be classed as a Trojan. In common use, most people (including Computer Knowledge) use Trojan to refer to a non-replicating malicious program.

Please visit our sponsors.

Click Here to Visit our Sponsor

AV Software | License | Virus Plural | Partition Sector | DOS Boot Sector | FDISK /MBR | False Authority | Logic Bombs | Trojans | Worms

Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats

Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small

payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.

[Pray the Rosary](#) for peace.

ccknow.com

Worms

Virus Tutorial

Click Here to Visit our Sponsor

Navigation

Misc. Terms

Tutorial Map

Anti-Virus Software

A worm is a self-reproducing program that does not infect other programs as a virus will, but instead creates copies of itself, and these create even more copies.

Worms are usually seen on networks and on multi-processing operating systems, where the worm will create copies of itself that are also executed. Each new copy will create more copies quickly clogging the system.

The so-called ARPANET/INTERNET "virus" was actually a worm. It created copies of itself through the network, eventually bringing the network to its knees. It did not infect other programs as a virus would, but simply kept creating copies of itself that would then execute and try to spread to other machines.

Some newer macro viruses also send their infected documents over the Internet to others who then infect their systems and spread the virus further. Some have classed these as worms. However, because these programs require a host in order to spread (even though they send themselves and the host over a network) Computer Knowledge (and most anti-virus researchers) puts these beasts into the virus category. But, you can see where distinctions between categories can get blurred.

The newer script worms don't help clarify the classification issue. Many of these are sent as a VisualBasic Script (VBS)

file attached to an E-mail message. If you click on the attachment to open it the script runs and will often send the script to addresses in your E-mail address book; thus spreading itself. Technically, these would be worms but are often called viruses.

Please visit our sponsors.

Click Here to Visit our Sponsor

AV Software | License | Virus Plural | Partition Sector | DOS Boot Sector | FDISK /MBR | False Authority | Logic Bombs | Trojans |
Worms
Virus Tutorial Home | Virus Intro | Virus Types | Virus History | Virus Protection | Virus Hoaxes | Current Threats
Home | Products | Definitions | Newsletter | Virus Tutorial | Contact

Help! Did you learn anything from these pages? Did they help you? If so, we are grateful and hope that you will be grateful also. Advertising only pays for a small percentage of the cost of maintaining this Web site. If you learned something and wish to help you can use the Amazon.com PayPage button below to send a small payment in return. Thank you in advance if you choose to do this.

Amazon Honor System

Send mail to webmaster@cknow.com with questions or comments about this web site.
Copyright © 2001 Computer Knowledge, All Rights Reserved
Pray the Rosary for peace.