DOCUMENT RESUME

ED 412 892	IR 018 338
AUTHOR	Ponder, Tim, Comp.; Ropog, Marty, Comp.; Keating, Joseph, Comp.
TITLE	Computer Viruses. Technology Update.
INSTITUTION	Kent State Univ., OH. Ohio Literacy Resource Center.
PUB DATE	1997-00-00
NOTE	5p.; Compiled from information from the Internet.
AVAILABLE FROM	Available on the World Wide Web at: http://literacy.kent.edu/oasis/pubs/0500-4.html
PUB TYPE	Reports - Descriptive (141)
EDRS PRICE	MF01/PC01 Plus Postage.
DESCRIPTORS	*Computer Networks; *Computer Security; Computer Software; Disk Drives; Floppy Disks; Information Sources; Information Technology; Microcomputers; *Prevention; Problems; Risk Management; Technical Assistance
IDENTIFIERS	*Computer Viruses; Data Security

ABSTRACT

This document provides general information on computer viruses, how to help protect a computer network from them, measures to take if a computer becomes infected. Highlights include the origins of computer viruses; virus contraction; a description of some common virus types (File Virus, Boot Sector/Partition Table Viruses, Trojan Horses, and Stealth Viruses); and prevention. A list of common virus symptoms and resources for technical support are included. (AEF)

O hio
L iteracy
R esource
C enter

039-0500-0004
MARCH 1997

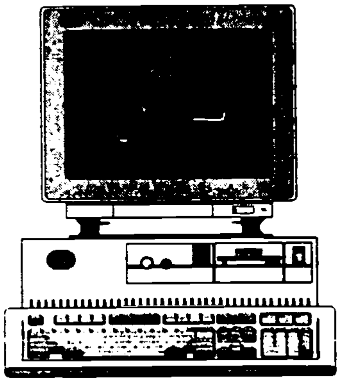
Enhancing adult literacy in the State of Ohio

TECHNOLOGY UPDATE

COMPUTER VIRUSES

COMPUTER VIRUS: reactions to hearing those words vary greatly. Too often, the reaction is one of two extremes. Either the computer users ignore the chance of a virus, or they become overly concerned to the point of not wanting to use the computer for fear of contracting a virus.

Computer viruses are very real threats. They can be simply annoying, requiring time to remove and clean up. On the opposite end of the spectrum, they can be very destructive, destroying data with little or no warning. Viruses are more prevalent today than ever, but so are tools and techniques to avoid them. To deal with viruses, a user needs to know a bit about them, practice a few good habits, run an effective anti-virus program, and know what to do if one does strike.



The first sections focus on general virus information. Following that is a list of things to do and not to do in order to help protect a computer or network as well as measures to take if a computer does become infected. The last section contains several resources to find more information.

ORIGINS OF COMPUTER VIRUSES

As recent as the mid-80's computer viruses did not exist. The first viruses were created in university labs - to demonstrate the "potential" threat that such software codes could provide. By 1987, viruses began showing up at several universities around the world. Three of the most common of today's viruses - STONED, CASCADE and FRIDAY THE 13th - first appeared that year.

Serious outbreaks of these viruses began to appear over the next two years. The DATACRIME and FRIDAY THE 13th viruses became major media events. Surprisingly, Bulgaria became known as the world's Virus Factory in 1990 because of the high number of viruses created there. The NCSA (National Computer Security Association) found that Bulgaria, home of the notorious Dark Avenger, originated 76 viruses that year, making it the world's single largest virus contributor. Analysts believe that Bulgaria's mass production of viruses is due in part to the abundance of well trained but unemployed programmers; with nothing to do, these individuals tried their hand at virus production, with unfortunately successful results.

This growing activity of virus production convinced the computer industry that viruses were a serious threat and defensive measures should be developed. IBM created its High Integrity Computing Laboratory to lead Big Blue's anti-virus research. Symantec, which began offering Symantec Anti-Virus, was one of the first commercially available virus defenses. This new technology came none too soon. By 1991, the first POLYMORPHIC viruses - that can, like the AIDS virus in humans, change their shape to elude detection - began to spread and attack in significant numbers. During that year, the total viruses began to swell, topping some 1,000 for the first time.

Virus Contraction

Viruses come from a variety of sources. Because a virus is software code, it can be transmitted along with any legitimate software that enters your environment.

- In a 1991 study of major U.S. and Canadian computer users by the market research firm Dataquest for the National Computer Security Association, most users blamed an infected diskette (87 percent). Forty-three percent of the diskettes responsible for introducing a virus into a corporate computing environment were brought from home.
- Nearly three-quarters (71 percent) of infections occurred in a networked environment, making rapid spread a serious risk. With networking, enterprise computing and inter-organizational communication on the increase, infection during telecommunication and networking is growing.
- Seven percent said they had acquired their virus while downloading software from an electronic bulletin board service.
- Other sources of infected diskettes included demo disks, diagnostic disks used by service technicians and shrink-wrapped software disks - contributing six percent of reported infections.

Technical Overview

Viruses are small software programs. At the very least, to be considered a virus, these programs must be able to replicate themselves. They do this by exploiting computer code already on the host system. The virus can infect, or become resident in, almost any software component, including an application, operating system, system boot code or device driver. Viruses gain control over their host in various ways. The following is a summary of some more common virus types, how they function, and how you can fight them.

File Virus

Most of the thousands of viruses known to exist are file viruses, including the FRIDAY THE 13th virus. They infect file by attaching themselves to a file, generally an executable file - the .EXE and .COM files that control applications and programs. The virus inserts its own code in any part of the file. Provided it changes the host's code, the program execution is misdirected so that it executes the virus code first, rather than the legitimate program.

Boot Sector/Partition Table Viruses

While there are only about 200 different boot sector viruses, they make up 75 percent of all virus infections. Boot sector viruses include Stoned, the most common of all time, and Michelangelo, perhaps the most notorious. These viruses are so prevalent because they are harder to detect, since they do not change a file size or slow performance, and are fairly invisible until their trigger event occurs - such as the reformatting of a hard disk. They also spread rapidly.

The boot sector virus infects floppy disks and hard disks by inserting itself into the boot sector of the disk, which contains code that's executed during the system boot process. Booting from an infected floppy allows the virus to jump to the computer's hard disk. The virus executes first and gains control of the system boot even before MS-DOS is loaded. Because the virus executes before the operating system is loaded, it is not MS-DOS specific and can infect any PC operating system platform - MS-DOS, Windows, OS/2, PC-NFS, or Windows NT.

The virus goes into RAM, and infects every disk that is accessed until the computer is rebooted and the virus is removed from memory. Because these viruses are memory resident, they can be detected by running CHKDSK to view the amount of RAM and observe if the expected total has declined by a few kilobytes. Partition table viruses attack the hard disk partition table by moving it to a different sector and replacing the original partition table with its own infectious code. These viruses spread from the partition table to the boot sector of floppy disks as floppies are accessed.

Trojan Horses

Like its namesake, the Trojan Horse virus typically masquerades as something desirable - like a legitimate software program. The Trojan Horse generally does not replicate (but some cases of replication have been discovered). This virus type generally waits for a triggering event like displaying a message or reformatting a hard disk before it performs the infection.

Stealth Viruses

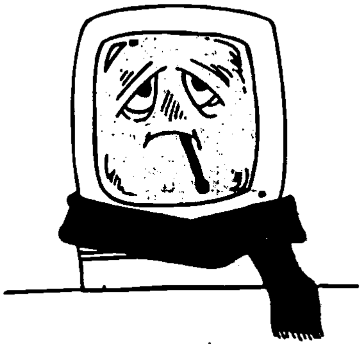
Stealth viruses have special engineering that enables them to elude detection by traditional anti-virus tools. The stealth virus adds itself to a file or boot sector but, when you examine the host software, it appears normal and unchanged. The stealth virus performs this trickery by lurking in memory when executed. There it monitors and intercepts your system's MS-DOS calls. When the system seeks to open an infected file, the stealth virus races ahead, uninfects the file and allows MS-DOS to open it - all appears normal. When MS-DOS closes the file, the virus reverses these actions, reinfecting the file.

Prevention

By following a few guidelines, the risk of contracting a virus can be minimized and chances of full recovery increased. First and most important is the purchase of a virus scanning program. These can be purchased at any store that sells software or computers. Some of the most common titles include: Dr. Solomon's Tool Kit, Mcafee Virus Scan, Norton Anti-Virus, and PC-Cillin. These programs are designed to help guard against viruses and remove and clean up after any virus infection. By following the setup instructions carefully and setting tasks to be automated wherever possible (such as automatically checking any file downloaded from the Internet), chances of getting a virus are greatly reduced. When purchasing an anti-virus program, there are three things to look for:

1. How well does it detect viruses?
   Most current programs do an excellent job of finding viruses.
2. How well does it clean up a virus?
   This is important as well. Can the program remove the virus from your system?
3. How does the user update the software?
   Viruses change often, and companies should have a good method for updating the software such as downloading from the web or frequent disk mailings. These should be included in the cost of the program or be available at a very modest cost.

In addition to any automated settings in a program, several other good habits are important. Scan all floppies that you receive from someone else, purchase, or use in any other computer. This is the most common way for viruses to spread. Disks that come from computer labs or office settings are more likely to be infected. If you are online, be sure to scan any files downloaded immediately after saving. Or, better yet, set your virus software to do this automatically. Another good habit is to be careful where you download from. Large sites such as www.shareware.com or software and hardware companies are generally safer. Individuals on the Web may not have taken as many precautions.



As mentioned, a virus is generally carried in programs that do something, such as zip, com, bat and exe files. However, a recent trend is to build them into macros, or small programs that can be included in word processing documents. Thus, it is a good ideas to scan *anything* downloaded, or any disk from someone or somewhere else. It is very rare that new software purchased will be infected. However, it is possible, and the few minutes it takes to scan can save days or weeks of "clean-up" time.

All of this will still not guarantee that a computer will not get a virus (although the odds become very small). If a virus is contracted, most virus programs will clean the infected disks. Here, thoroughness in cleaning is the key. Be sure to clean the hard drive as well as any floppy disks that may have been used while the computer was infected. Also, if you used the disk on any other computer, let that computer's owner and other users know. If you feel you know where you contracted the virus, contact the appropriate people and inform them that their machine or machines could be infected. This is where having a recent backup can be extremely valuable. Frequent backups of data files may be lifesavers if a particularly ornery virus strikes. When installing virus software, be sure to read and follow the directions for making a boot disk. This way, if a drive is infected, the computer can be started "clean" from a floppy. This is necessary since once a computer is started from an infected disk, the virus can then "hide" from any anti-virus software.

The threat of computer viruses should not be ignored. However, with a few simple steps, some software and good habits, the threat can be nearly eliminated. Following are several additional resources. As always, feel free to contact the technical support staff at the OLRC.

• Symantec Anti-Virus Research Center	www.symantec.com/avcenter
• Virus and Anti Virus Help	www.cadvision.com/reinwarw/eaglevir.htm
• NCSA (National Computer Security Association)	www.ncsa.com
• Computer Virus Myths (Not bad, but has two mistakes on it)	kumite.com/myths

Common Virus Symptoms (From http://server.snni.com/~robertc/virus.html#clean)

- Hard Drives using MS-DOS compatibility mode in Windows 95.
- Unable to read Disk 2 of Windows 95 Diskettes.
- 32 bit File Access doesn't work in Windows.
- The CMOS forgets its settings even with a new battery.
- Program size keeps changing.
- Can't access the hard drive after booting from a floppy.
- Programs or Windows takes longer to load.
- CHKDSK reports less than 655360 bytes available.
- Clicking noises from the PC speaker while typing.
- You see strange messages.
- Windows crashes.
- Files keep getting corrupted.
- Your hard drive becomes a single encrypted zip file.
- You start to find strange files on your drive.
- Letters fall to the bottom of the screen.
- Hard drive keeps running out of free space.
- The drive light flashes for no reason.
- HDD Controller Failure message

Compiled by Tim Ponder, Marty Ropog and Joseph Keating from information from the Internet

THE OHIO LITERACY RESOURCE CENTER IS LOCATED AT KENT STATE UNIVERSITY
414 WHITE HALL, P.O. BOX 5190, KENT, OH 44242-0001
1-800-765-2897 OR 330-672-2007
E-MAIL ADDRESS: OLRC@LITERACY.KENT.EDU

U.S. Department of Education
Office of Educational Research and Improvement (OERI)
Educational Resources Information Center (ERIC)

ERIC®

REPRODUCTION RELEASE

(Specific Document)

I. DOCUMENT IDENTIFICATION:

Title: Ohio Literacy Resource Center Technology UPdate: Computer Viruses

Author(s): Compiled By: Joseph Keating, Tim Ponder, Marty Ropog

Corporate Source: Ohio Literacy Resource Center

Publication Date: 3/1997

II. REPRODUCTION RELEASE:

In order to disseminate as widely as possible timely and significant materials of interest to the educational community, documents announced in the monthly abstract journal of the ERIC system, *Resources in Education* (RIE), are usually made available to users in microfiche, reproduced paper copy, and electronic/optical media, and sold through the ERIC Document Reproduction Service (EDRS) or other ERIC vendors. Credit is given to the source of each document, and, if reproduction release is granted, one of the following notices is affixed to the document.

If permission is granted to reproduce and disseminate the identified document, please CHECK ONE of the following two options and sign at the bottom of the page.

☒

Check here
For Level 1 Release:
Permitting reproduction in microfiche (4" x 6" film) or other ERIC archival media (e.g., electronic or optical) *and* paper copy.

The sample sticker shown below will be affixed to all **Level 1** documents

PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL HAS BEEN GRANTED BY

Sample

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

Level 1

The sample sticker shown below will be affixed to all **Level 2** documents

PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL IN OTHER THAN PAPER COPY HAS BEEN GRANTED BY

Sample

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

Level 2

□

Check here
For Level 2 Release:
Permitting reproduction in microfiche (4" x 6" film) or other ERIC archival media (e.g., electronic or optical), but *not* in paper copy.

Documents will be processed as indicated provided reproduction quality permits. If permission to reproduce is granted, but neither box is checked, documents will be processed at Level 1.

"I hereby grant to the Educational Resources Information Center (ERIC) nonexclusive permission to reproduce and disseminate this document as indicated above. Reproduction from the ERIC microfiche or electronic/optical media by persons other than ERIC employees and its system contractors requires permission from the copyright holder. Exception is made for non-profit reproduction by libraries and other service agencies to satisfy information needs of educators in response to discrete inquiries."

Sign here→ please

Signature:

Printed Name/Position/Title: TIM PONDER Asst. Director

Organization/Address:
Ohio Literacy Resource Center
414 White Hall
Kent State University
Kent OH 44242

Telephone: 330-672-2007

FAX: 330-672-4841

E-Mail Address: tponder@literacy.kent.edu

Date: 10/24/97

(over)

III. DOCUMENT AVAILABILITY INFORMATION (FROM NON-ERIC SOURCE):

If permission to reproduce is not granted to ERIC, *or*, if you wish ERIC to cite the availability of the document from another source, please provide the following information regarding the availability of the document. (ERIC will not announce a document unless it is publicly available, and a dependable source can be specified. Contributors should also be aware that ERIC selection criteria are significantly more stringent for documents that cannot be made available through EDRS.)

Publisher/Distributor:

Address: Available on the WWW at
http://literacy.kent.edu/Oasis/Pubs/0500-4.html

Price:

IV. REFERRAL OF ERIC TO COPYRIGHT/REPRODUCTION RIGHTS HOLDER:

If the right to grant reproduction release is held by someone other than the addressee, please provide the appropriate name and address:

Name:

Address:

V. WHERE TO SEND THIS FORM:

Send this form to the following ERIC Clearinghouse:

ERIC / IT
Center For Science & Technology
Room 4-194
Syracuse University
Syracuse, NY 13244-4100

However, if solicited by the ERIC Facility, or if making an unsolicited contribution to ERIC, return this form (and the document being contributed) to: