

Virus Alert

Computer viruses

virus: *n.* A self-replicating program containing code that explicitly copies itself and "infects" other programs by modifying them or their environment such that a call to an infected program implies a call to a possibly evolved copy of the virus.

worm: *n.* A program that propagates itself over a network, reproducing itself as it goes.

Viruses infect programs by incorporating themselves into the program itself. Some viruses, like the "Trojan Horse", cannot activate themselves without attaching to another program. The virus then replicates and executes the legitimate program's coding.

There are many ways to write viruses. Some of the most common are:

1. Overwriting the beginning of a file to infect a program with the virus' coding. This method however, may only cause the program to run improperly. When the computer reaches the end of the viral coding it will return to the code left before the introduction of the virus. This creates errors by segueing the start-up functions of the infected program.
2. Adding a jump to the end of a program where the viral code is located, and then continuing with a jump to the beginning of the program where it left

off. This kind of virus should not crash the program, but will decrease memory.

3. Appending the virus to the beginning of the program without altering the program's original coding.

Viruses are software programs that misguide the computer system by abusing the system's resources. Computer viruses work similarly to biological viruses. Biological viruses use their genetic code to take over the mechanics of a living cell and trick it into producing replicas of the original virus.

A well-written virus can delete or re-partition a computer's hard-disk by writing false values in the BOOT SECTOR or FAT (File Allocation Table). It can also tamper with the format of a hard-disk and delete files, thus corrupting the system's resources. The damage caused by a virus is capable of causing irreparable damage to the computer's system. Viruses modify the disk or file they attach themselves to. These modifications are similar with most viruses. We identify the virus by isolating a particular modification indicative to that virus' presence. This identified modification is the virus' *signature*. This signature consists of a unique string of characters. This unique string alerts the system to the presence of a virus.

Some viruses are capable of creating new viruses. These new, modified, viruses alter their signatures and methods of infection, thus producing a new *strain*.

Types of Viruses

Boot Sector viruses:

Boot Sector is infected or overwritten and a copy of the original boot sector is placed elsewhere on the disk. The virus code itself is placed in the Boot Sector or in sectors marked bad. These viruses take control of the system at the

Types of Viruses...continued on page 2

IN THIS ISSUE...

Computer Viruses.....	1
Types of Viruses	1
Prevention	2
Signs of attack	2
Hoax Viruses	2
The "I Love You" Worm	3
Can I get a virus from legitimate programs?	3
Is it true that a Virus or Worm can steal my Passwords?	3
One Last Look	4

Advertise with Liberty Computing Center

For more information call: 718-788-1086
Or visit: LibertyComputingCenter.com

time of the system's boot and inflict heavy damages thereafter. This may render the Boot Sector inoperable.

Partition table viruses:

These viruses reside at the partition table and gain control of the machine when the boot loader executes the code that is used by the active partition table.

File viruses:

These viruses attach themselves with *.EXE and *.COM files. The command processor i.e. COMMAND.COM (the basic user interface of the Disk Operating System) is usually effected first, and typically the damage demands deletion of the infected files.

Macro viruses:

Macro is defined as a sequence of tasks that can be specified in a package like Word. For example, the macro can convert the sequence of a list from "last name to first name" into "first name to last name".

Macro viruses such as the infamous Melissa virus can infect Word documents, email programs, etc. If a macro virus is found, the macros are to be disabled to avoid further corruption.

Prevention

Your first step in prevention is use of a reliable virus-scanning program. It is recommended that two be applied. It is preferable to use a scanner that remains in the system's memory, this will check all files and memory prior to opening them. This also applies when reading a floppy disk; make certain to always scan any floppy disk you read. Finally, it is imperative that all downloads are scanned. The majority of viruses are activated through a tainted program downloaded from the Internet, or through email. If you receive an email from an unknown source, delete it immediately. If the email contains an attachment, DO NOT open or execute the program. If you have already double-clicked and executed the attachment, immediately scan all system disks and files. For best results check your scanner manufacturer's website on a daily or weekly basis to insure you have the latest data file for your scanner.

You can find more information at: www.symantec.com
or
www.mcafee.com

Signs of Attack

In some instances it is very apparent when your system has been infected with a virus. In other cases the infection may not surface until considerable damage has taken place, so prevention is the most effective method of protection. Some of the telltale signs of a virus are:

Signs of Attack...continued on page 3

Hoax virus says trash Windows file

hoax: *n.* To trick into believing or accepting as genuine something false and often preposterous. In other words, a virus that does not exist but creates panic because of heavy promotion.

The email, which was originally written in Portuguese and was reported to be making the rounds in Brazil last month, has been translated to English and is circulating in the United Kingdom. Recipients are advised to delete a harmless Microsoft Windows utility called *sulfnbk.exe* from their hard disks.

Antivirus experts were quick to point out that the email does not contain a worm or a virus and is being passed around by well-meaning people warning others of the alleged virus. As a result, it cannot be detected by virus-scanning software or junk email filters. When users receive this warning and delete the file from Windows, they are effectively doing the work of a deadly virus.

The hoax message indicates that the virus is scheduled to trigger June 1, and has been found on every PC. In fact, the file *is* on every PC that has Windows installed and is not detected by anti-virus software because it is not a virus. The file that people are being asked to delete is a legitimate file that is part of the Windows operating system.

Sulfnbk.exe is a Microsoft Windows utility that is used to restore long file names, and deleting it could cause that feature to stop working properly. The confusion may have been heightened by the fact that emails were surfacing that contained a copy of the *sulfnbk.exe* file that was infected with a virus. This virus, called *W32.Magistr.24876@mm*, is well known and easily removed with any good anti-virus software.

It has been hypothesized that the new email was started by someone who was forwarded a message by a colleague whose PC did actually have the *Magistr worm*. This person may have searched for the *Sulfnbk.exe* file, found and

Hoax Virus...continued on page 3

NEXT ISSUE:

Recreation and Technology

Publisher: Liberty Computing Center, Inc.

Editor in Chief: William M. Brandon III

Editor@LibertyComputingCenter.com

Production Manager: Daniel Ramos

Dramos@LibertyComputingCenter.com

For more information visit:

LibertyComputingCenter.com

- Sluggish computer system.
- Programs take longer than normal to load.
- Programs access multiple drives.
- Programs conduct disk access with increased frequency.
- Available disk space decreases rapidly.
- Available RAM decreases.
- Programs function abnormally or crash without reason.
- Programs generate undocumented messages.
- Black holes, bouncing balls, smiling faces appear on screen.

deleted it (after discovering that anti-virus software failed to recognize the file), and sent a warning to other users.

There are several easy clues to detect bogus virus warnings. Anything that has lots of capital letters saying things like VIRUS WARNING should be treated with skepticism. In addition, phrases warning that a supposed virus will absolutely destroy everything on a hard disk should be taken lightly, as well as those suggesting there is no known cure. Hoax emails also often attribute information to MSN, AOL, Microsoft, and CNN to give them credibility, but these companies don't usually issue virus warnings.

The hoax email begins as follows:

"URGENT. A VIRUS could be in your computer files now, laying dormant but will become active on June 1, 2001. FOLLOW DIRECTIONS BELOW TO CHECK IF YOU HAVE IT AND HOW TO REMOVE IT NOW.

It was brought to my attention that this virus is in circulation via email. I looked for it and to my surprise I found it on my computer as well as everyone else's in my office. Please follow the directions and remove it from yours TODAY!!!!!!!"

The email then goes on to give a detailed list of instructions on how to delete the *sulfbnk.exe* file.

Can I get a virus by installing a legitimate program?

Yes. It is rare to receive a virus from programs straight out of the manufacturer's box, but it does occur. Most software companies perform extensive tests for viruses before releasing the product, but oversights can occur. Make certain to *always* scan thoroughly *any* program you introduce into your system.

Is it true that a virus or worm can steal my password?

Yes. A new strain of the 'I Love You' virus appears to have first affected the United Bank of Switzerland's European operations. In a release the company said that only "a small proportion of UBS e-banking customers are at risk" and that "there are no reports of damage as of yet." The Swiss bank said it has installed virus filters that have "successfully prevented the virus from spreading within UBS." The new strain downloads and runs a program, "hcheck.exe," that steals passwords from an infected computer. While the virus is at work, people see a résumé for "Knowledge Worker, Zurich," written in German.

Where can I learn more about Computer Viruses?

Virus Proof

by Phil Schmauder
ISBN: 0761531920

find it at SaveByClicking.com

The "I Love You" Worm

The "I Love You" worm is sweeping across the world. The worm, which targets users of Microsoft Outlook, comes in the form of an email with the subject line "ILOVEYOU" and an attachment named "LOVE-LETTER-FOR-YOU.TXT.vbs," which is a Visual Basic file. Running the file executes the worm. If you're unfortunate enough to execute the "LOVE-LETTER-FOR-YOU.TXT.vbs" file, the worm will send copies of itself to every person listed in your Outlook address book. It also overwrites any existing local script and HTML files, as well as .jpg and .jpeg files with its own code. It marks .mp3 and .mp2 files as hidden and creates replicas of itself in their place.

Note: There have also been sightings of the same virus coming in emails with the subject "Fwd: Joke" and the attachment named "VeryFunny.vbs." Another variation of the virus has the words "Susitikim shi vakara kavos puodukui..." in the subject line, while still another reads "Mothers Day Confirmation Order" in the subject.

How many viruses are known and how do I find more information concerning viruses?

For information: <http://dispatch.mcafee.com/>
Virus Information Library: <http://vil.mcafee.com>

United Internet Services Inc. in conjunction with Liberty Computing Center due to launch a High Tech Incubator in Brooklyn, New York.

For more information about this and other projects please visit:

LibertyComputingCenter.com/incubator.htm or call: 718-788-1086

The Incubator will look for companies with strong technology offerings such as computer consulting, ISP, Technical service, programming, e-commerce, communication, and other products and services with breaking technology. The center will be the ideal launching pad for entrepreneurs and inventors looking to develop innovative services and products while maintaining a low overhead in the critical startup stages.

For more information visit: <http://LibertyComputingCenter.com/incubator.htm> or call: 718-788-1086

Can't afford a full time computer specialist? Are you paying big bucks to a technician who spends most of his/her day playing solitaire on your system? If you answered YES to any of the above questions, then outsourcing is your solution to getting the job done at the right price. Liberty Computing Center. provides computer outsourcing for all of your needs. From recommending which computer is best for your needs to setting up complicated networks and giving you Internet presence with e-commerce accounts and shopping carts.

Outsourcing: <http://LibertyComputingCenter.com/Outsourcing.htm>

We offer a variety of computer training programs to help individuals, non-profit organizations, small businesses and corporate America understand the needs and the know-how of today's information technology demand.

Training: <http://LibertyComputingCenter.com/training.htm>

One last look...

Matchmaker virus spreading

A computer virus disguised as a matchmaking program was still spreading Thursday from its British hatching ground, with more than 1,000 PCs infected in South Africa and a few dozen in Australia and New Zealand. The virus, known as "Matcher.A" or "Bugger," arrives as an email attachment disguised as a program for finding romantic mates. The email says the following: "Want to find you love mates!!! Try this it's cool...Looks and Attitude Matching to opposite sex." The virus, which affects only Windows PCs, does not harm the infected computer but could overwhelm email servers as it spreads. Once activated, the virus periodically sends identical messages to everyone in a victim's address book.

Liberty Computing Center
P.O. Box 320
Brooklyn, NY 11215