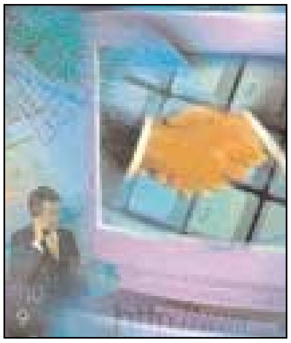
THE MALICIOUS LOGIC BATTLE: UNDERSTANDING THE ENEMY

By Julie Lucas

ENTERASYS NETWORKS™

Table of Contents



Known as virus, worm, Trojan horse and logic bomb, malicious logic robs productivity and jeopardizes every organization's information security and infrastructure. These computer programs, written with spiteful intent, perform unauthorized routines to damage and destroy data, or degrade system performance. Though the level and type of damage varies, the impact can be enormous with the greatest costs usually tallied in man-hours expended on recovery.

There is virtually no way to keep an organization completely free from malicious logic. However, there are steps everyone can take to proactively address the problem. First, one must understand the types of codes and recommended courses of action.

The Familiar Computer Virus

Of all the forms of malicious logic programs, the one that is familiar to most people is the computer virus. A virus is a self-replicating program whose purpose is to propagate to as many different places as possible. Viruses do this by modifying other programs to include copies of themselves through an (unknowing) act of a user.

Although viruses have received much attention from the media in recent years, they have actually been in existence since 1980. In his thesis written in 1984, Fred Cohen termed the phrase "computer virus" because of its similarity to a biologic virus, which replicates its DNA.

What's In A Virus' Name?

A virus is normally named based on some function it performs or a name that is used in its "signature." Frequently, virus writers will change an existing virus slightly and re-release the modified code to create a new strain. These "new" strains are usually identified with the original virus name and an alphabetic extension. For example, Wazzu, the original name of a com-mon macro virus, was modified several times for "new" variations denoted as Wazzu.A, Wazzu.B, and so on.[2]

The new strains of existing viruses account for the large population explosion of computer viruses over the years. In 1992 and 1993, the average number of new computer viruses per month was between 100 and 150.[3] Most of these "new" viruses were not actually brand new viruses, rather they were new strains of existing viruses. In January 1997, the average number of new discoveries was at 200 per month with a total of more than 8,500 known computer viruses. The numbers have continued to rise with time and in October 1999, Symantec released an updated signature file for their Norton Anti-Virus software that increased the number of detected viruses by 646 in just 4 days!

[2] Skardhamar, p.12.

[3] Skardhamar, p.12.

The following chart from Virus Detection and Elimination by Rune Skardhamar compares computer and biologic virus characteristics. [sic]:[1]

Computer Virus	Biologic Virus
Computer viruses are parasitic. They need another program to exist in and reproduce.	Biologic viruses are parasitic. They need a cell in which to live and reproduce.
Once a program has been infected it is forced to make new copies of the virus.	Once a cell has been infected, the infected cell is forced to make new copies of the virus.
Computer viruses are seldom used to infect the same program/disk twice.	Biologic viruses rarely, if ever, infect same cell twice.
Specific computer viruses target specific program types (exe, com, sys, boot record, etc).	Specific biologic viruses target specific cell types.
An infected program does not always show an obvious sign of the infection.	An infected cell can go on living for a long time without any obvious sign of infection.
After an incubating time of varied length, a computer virus often releases some kind of payload, which can prove fatal to the whole system.	After an incubating time of varied length, a biological virus often releases some kind of payload, which can prove fatal to the whole living system in which the infected cell lives.
A typical computer virus has a size of some 1,000 to 3,000 bytes. However, if the DOS interrupt sub routine is added to that, the size can easily be multiplied by two.	The DNA of a typical small virus, such as the polio virus, contains information that if reproduce on a computer would add up to some 5,000 bytes. The smallest virus discovered to date is equal to about only 200 bytes.

Five Main Virus Types

Overall, there are five main types of computer viruses: file infectors, partition-sector viruses, boot sector viruses, companion viruses, and macro viruses. The type of virus is determined by the methods used for propagation.

- **File infectors replicate** by inserting themselves into executable files. Usually, the virus code is written at the beginning of a targeted file, so it is executed immediately, or appended to the end. If the code is written somewhere other than the beginning of the file, the startup sequence of instructions in the file is normally modified to transfer program control to the malevolent code.

- **Partition-sector infectors** contaminate the partition record of a hard disk. First, the virus copies and stores the whole partition somewhere else on the hard disk. Then the virus copies itself to the partition sector and executes when the computer is booted from the hard drive.

- **Boot sector viruses** infect both floppy diskettes and hard disks by changing or replacing the boot-sector program with a copy of itself. This type of virus is most frequently spread by forgotten floppy diskettes left in disk drives. It can be considered a special case of the file infector virus, which only infects the boot-sector program.

- **The companion virus** searches for executable programs with the .exe or .bat extension, and creates a copy of itself with the same name, but with a .com extension. The virus is executed when a user tries to execute the legitimate file from the command line. After the virus completes its routine, control is returned to the original file. Companion viruses tend to spread only within a computer system and are normally easy to spot through both manual and automatic means.

- **Macro viruses** were discovered in the summer of 1995. Instead of infecting an executable program file or disk boot sector, the virus infects an application's document files. The virus contains a set of application-specific macro commands that automatically execute in an unsolicited manner then spread to the application's documents.

In addition to these types or categories of viruses, two additional definitions frequently used to describe viruses are multipartite and polymorphic. A multipartite virus combines two or more different infection methods, and a polymorphic virus changes itself with each virus infection. The polymorphic virus normally includes some sort of "mutation engine" to change itself during an infection in an attempt to elude detection.

[1] Skardhamar, Rune Virus Detection and Elimination. Academic Press Inc., 1996, p.14, sic

Typical Symptoms

Symptoms indicating the presence of a computer virus vary. Some of the typical signs indicating a virus may be present include:

- Display of an unusual message
- Missing files
- Files with increased size
- A slowdown in the operation of the computer
- Sudden lack of disk space
- The inability to access the disk drive. These symptoms may be attributed to other problems as well, so one should not assume the problem is automatically a virus without further investigation.

Melissa, An Infamous Macro Virus

Melissa, a macro virus released on March 26, 1999, was first discovered on an "alt.sex" newsgroup. By targeting machines running Microsoft Word 97 or Word 2000, it spread rapidly through e-mail attachments to computers worldwide. Once an infected attachment was opened, the virus would propagate by sending an e-mail with another infected attachment to the first 50 addresses in the victim's address book. Since the e-mail appeared to come from the victim, a "trusted source," recipients would open it and get caught off guard. Damage was higher than any previous virus. A complete description of the Melissa virus with detailed course of actions can be obtained from http://www.cert.org/advisories/CA-99-04- Melissa-Macro-Virus.html as well as several other sources.

The System Administration, Networking, and Security (SANS) Institute provided a flash report concerning the infection on March 29, 1999, which provides an excellent account of how the virus caught people by surprise. The following is an excerpt:

A network engineer at one of the first sites to report the problem last Friday March 26, said "I knew something was wrong before I knew what was wrong. I could feel the network going slower and slower. As I looked into it, I found the exchange mail servers were melting down." One of the lessons of Melissa is that a macro virus can hit very fast and very hard. The engineer went on to say, "As I composed the last email of the day, a message hit the Inbox of my Microsoft Outlook email application. The subject line read: "Important Message From [Jane Doe]." I viewed the message, and the body read "Here is that document you asked for... don't show anyone else :-)" Attached was a Microsoft Word docu-ment titled "list1.doc."

"Although I hadn't requested any documents from [Jane Doe], I expected a couple of them from other people. It wasn't inconceivable that she had become involved, even though I didn't know who she was. I double-clicked on the Word document. A pop-up window appeared, warning me that a macro was contained in the document, and that macros can potentially be dangerous. I knew that... :-) So, I shut down the Word application, and checked the document with several virus detection packages. Everything appeared clean."

"Since this was from someone in my organization, apparently a trusted source, I went ahead and opened the document with the macros enabled. In less than a second, a duplicate of the message hit my mailbox, this time with my name attached. I hit the power-off button on my computer, but it was too late. The payload had been delivered. My name was now attached to a file containing pornographic web sites, and an apparent user-name and password for each site. Moments later, duplicate messages from others who had made the same mistake began to appear."

"At this point I knew we, as an organization, were in trouble. This virus was snowballing fast, too fast. I immediately called our information systems security manager, only to find that his phone was already busy. I left a voicemail detailing my appraisal of the situation and my fear that this incident could get serious... very quickly. What I didn't know was that I was too late, it was already *very* serious."[4]

[4] http://www.sans.org/newlook/resources/IDFAQ/What_Melissa teaches_us.html

Viruses Prey on User Trust to Propagate

After Melissa, it became even more apparent that end user awareness and education is one of the greatest weapons against loss. People need to know why Melissa spread so rapidly. Though wide spread use of the Microsoft Word platform delivered the targets, user trust made it possible for the virus to infect each system's address book and propagate. A snowball effect was quickly attained thanks in part to group addresses and list servers, which enabled the code to spread to multiple recipients at once.

The wide spread use of the Microsoft Word platform provided several targets to continue the virus' spread. If the Word application had not previously been infected by a virus, then the pop-up box reflecting the presence of a macro should have appeared when an infected file was opened. A user who indicated the macro should not be opened would not have fallen victim to the virus. However, those that did permit the macro to run were added to the list of victims. The security feature the "pop-up macro warning" provides should be included in virus awareness training.

Fast Response Saved the Day

In addition to demonstrating how quickly a virus spreads, Melissa was an example of how rapidly and thoroughly the computer security community can respond. For instance, signature files for anti-virus software products were quickly updated. Immediate advisories, bulletins, and media announcements alerted computer users worldwide. Around the world, numerous system administrators worked long hours to contain the virus and clean code within infected networks. The computer incident response community joined forces to share reported symptoms and provide accurate problem assessment. The entire community can be credited for a job well done.

Ultimately, a particularly nasty virus may escape detection and cause the loss of critical data on workstations or file servers. In those situations, a conscientious file backup program is absolutely essential. Even if the virus code is backed up on the tape or other media, system administrators can update virus definitions to remove it. The code will not run until the operating system is running again, thus restoration of data onto a new PC updated with anti-virus protection becomes possible.

Important Steps to Remain Virus Free

Regardless of the type of virus, there are some basic steps that can go a long way to ensure your computer system remains virus free.

- Document and share standard "anti-virus" procedures.
- Train users to consistently follow standards.
- Conduct regular scans with anti-virus software.
- Update anti-virus software as new signature files are available from software vendors.
- Use anti-virus software at various levels within the information infrastructure.
- Keep computer user's informed of the latest threats.
- Remind end users not to open unknown e-mail attachments with out first scanning for viral code.
- Do not leave diskettes in floppy drives when computers are turned off.
- In Microsoft Word applications the global template, typically a file called Normal.dot, should be scanned for viruses and set to read only.
- Any auto-run and auto-open features on e-mail programs and browsers should be disabled.
- The CMOS boot sequence could be changed to start with the C drive first, then A.

[5] Russell, Deborah and G.T. Gangemi Sr. Computer Security Basics. O'Reilly & Associates, Inc., 1991, p. 426.
[6] Skardhamar, p.15.

Other Forms of Malicious Logic

- A **worm** is "an independent program that reproduces by copying itself from one system to another, usually over a network. [5] Like a virus, a worm may damage data directly or it may degrade system performance by tying up resources and even shutting down a network." The worm written and released by Robert Morris, Jr. in late 1988 and the LoveLetter. VBS are examples.
- A **Trojan horse** is a program or routine concealed in software that appears to be harmless. Trojan horses are not viruses and do not replicate like viruses. However, they may contain or include a worm or virus as part of the package. The most common way to remove a Trojan horse is to simply delete the identified Trojan application. Trojan horses are quickly becoming one of the top security threats to computer systems. Back Orifice, Back Orifice 2000 (or BO2K), and Netbus are all examples of Trojan horses.
- A **logic bomb** is a software program that is triggered by a timing device (e.g., a date or event) to launch its payload. The payload may release a virus or worm, or perform some other type of attack. This is a popular device for disgruntled employees.

Most anti-virus software vendors try to include worms and Trojan horses in their signature strings, but the success rate of detection and eradication varies greatly. System administrators cannot assume the anti-virus software will detect and solve all malicious code problems.

Hoaxes and Legends Prey on Users' Goodwill

"A virus' true prey is not the computer, but the good will and ignorance of the users."[6] Similarly, virus hoaxes and urban legends prey on users to spread fear throughout the Internet.

Virus Hoaxes

A virus hoax is an e-mail warning of some "new" virus rumored to be in circulation on the Internet. Some of the warnings are very well written and convince well-intentioned users to forward them to others. Unfortunately, mass forwarding of the false e-mail spreads panic and productivity suffers. (Not to mention time wasted debunking false allegations, reading bogus postings, and tying up resources with multiple forwards of group mail.)

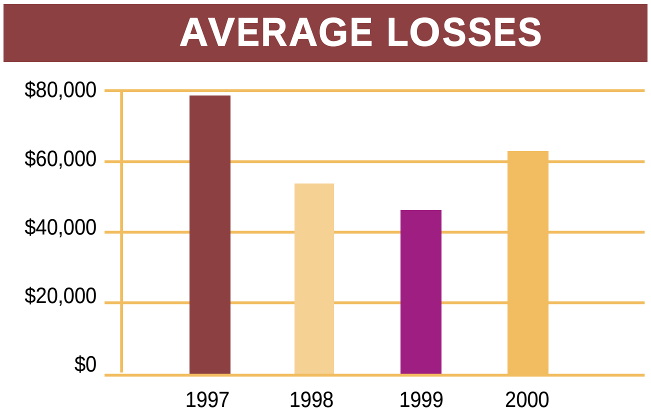
Urban Legends

Urban legends are very similar to virus hoaxes, except they forward a warning about some other major event, problem, or impending catastrophe. The story that aired on Dateline in late 1999 about the use of suntan lotion causing blindness in children is an excellent example of an urban legend. There are several Internet resources that may be used to confirm if a story is a virus hoax or urban legend. One of the best sites is http://www.vmyths.com/.

The bottom line – do not e-mail virus hoaxes or urban legends. If in doubt, check with a reliable source regarding their validity before taking any further action. The safest action is to press the delete key. Some organizations have experienced serious system performance degradation when well-intentioned users forward warnings to multiple sites. It is far better to leave the warnings to the experts, than to try and spread the "word," which only adds to the hype and may hurt one's integrity in the process.

Total Cost of Viruses Escalate

For the past five years, the Computer Security Institute (CSI) in conjunction with the Federal Bureau of Investigation has conducted a Computer Crime and Security Survey as a public service to increase computer security awareness and assist in determining the extent of computer crime in the United States. A total of 586 respondents indicated they had quantified losses due to computer viruses in the 1997 through 2000 surveys. The following graph depict the average loss reported in these surveys.



The total annual losses reported due to computer viruses were:

- 1997: $12,498,150 - 165 organizations
- 1998: $ 7,874,000 - 143 organizations
- 1999: $ 5,274,000 - 116 organizations
- 2000: $29,171,700 - 162 organizations

Although these figures may seem quite high, they are actually considered low due to the difficulty in trying to equate cost for a computer incident or crime. In fact, 74% of the respondents to the 2000 survey acknowledged they incurred financial losses due to computer crime, yet only 42% were able to quantify those losses. Typically, the financial loss attributed to virus infections is counted in labor hours expended while cleaning up the infection.

Winning the Battle--For the Next Virus

Computer viruses rob workers of productivity, redirect the attention of system administrators from more severe security threats, and can jeopardize the security of the organization's information infrastructure. Yet, there is virtually no way to completely keep an organization free from the viral code. To keep the problem in perspective, that is one of a nuisance more than a major threat, an organization must take steps to proactively address the problem. The first step that should be taken is increasing the overall awareness level of all end users. Addressing topics such as the importance of the macro warning box in Microsoft Word applications and the need to scan attachments for malicious code prior to opening them can go a long way in eliminating large-scale infections. Increased awareness will also help eliminate problems attributed to the virus hoaxes. In conjunction with awareness education, implementing anti-virus software throughout the enterprise with automatic updates of signature files remains the best course of action to combat viruses to date. The signature file updates may be programmed to occur during off-peak hours if desired. Whenever possible, the use of anti-virus software and the signature file updates should be implemented in a way that cannot be bypassed by end users. Finally, a check of configuration settings should be made to ensure auto-open features are disabled and global templates are set to read-only access. These two changes alone may help reduce the success level achieved by the next rapidly spreading virus. By implementing a proactive anti-virus program, the effects of malevolent code can be greatly minimized and organizations can start winning the malicious logic battle.

North America

35 Industrial Way
Rochester, NH 03867
U.S.A.
(603) 337-1600

50 Minuteman Road
Andover, MA 01810
U.S.A.
(978) 684-1000

Europe/Middle East/Africa

Network House
Newbury Business Park
London Road, Newbury
Berkshire, England RG13 2PZ
44-1635-580000

Asia Pacific

85 Science Park Drive
#03-01/04
The Cavendish
Singapore 118259
65-775-5355

Unit 10, 14A Rodborough Road
Beacon Business Park
Frenchs Forest NSW 2086
Australia
61-29950-5900

Latin America

Periferico Sur No. 3642
Piso 6
Colonia Jardines del Pedregal
Mexico City DF
Deleg. Alvaro Obregon
C.P. 01900
Mexico
525-490-3400

Av Nações Unidas, 12.551,
18º Floor
Brooklin-São Paulo
04578-903-Brazil
55-11-5508-4600