Anatomy of Computer Viruses

Even after you have read this, there will be a few who *must* open that email attachment to see what it is, or go to that enticing web site to get that “Free” thing! You're the "clickers" that have a *need* to see what it is. You can't help it! And when you left-click - telling it to do whatever damage it was designed to do - please don't be dismayed when you've lost programs, important data, your Quicken files, all your banking info, pictures of your loved ones, and all the saved stuff in My Documents. After all, *you* were the one who *told* it to do the damage, so *you* pay the price. The software or technician will do their best to restore what they can. See also HowStuffWorks!

Computer viruses are mysterious and grab our attention. On the one hand, viruses show us how vulnerable we are. A properly engineered virus can have an amazing effect on the worldwide Internet. On the other hand, they show how sophisticated and interconnected human beings have become.

For example, the things making big news right now are the MSBlaster worm and the SoBig virus. The Melissa virus - which became a global phenomenon in March 1999 - was so powerful that it forced Microsoft and a number of other very large companies to completely turn off their email systems until the virus could be contained. The ILOVEYOU virus in 2000 had a similarly devastating effect. That's pretty impressive when you consider that the Melissa and ILOVEYOU viruses are incredibly simple.

In this article, we will discuss viruses - both "traditional" viruses and the newer e-mail viruses - so that you can learn how they work and also understand how to protect yourself. Viruses in general are on the wane, but occasionally a person finds a new way to create one, and that's when they make the news.

Types of Infection - When you listen to the news, you hear about many different forms of electronic infection. The most common are:

1. Viruses - A virus is a small piece of software that piggybacks on real programs. For example, a virus might attach itself to a

program such as a spreadsheet program. Each time the spreadsheet program runs, the virus runs, too, and it has the chance to reproduce (by attaching to other programs) or wreak havoc.

2. E-mail viruses - An e-mail virus moves around in e-mail messages, and usually replicates itself by automatically mailing itself to dozens of people in the victim's e-mail address book.

3. Worms - A worm is a small piece of software that uses computer networks and security holes to replicate itself. A copy of the worm scans the network for another machine that has a specific security hole. It copies itself to the new machine using the security hole, and then starts replicating from there, as well.

4. Trojan horses - A Trojan horse is simply a computer program. The program claims to do one thing (it may claim to be a game) but instead does damage when you run it (it may erase your hard disk). Trojan horses have no way to replicate automatically.

What is a "Virus?" - Computer viruses are called viruses because they share some of the traits of biological viruses. A computer virus passes from computer to computer like a biological virus passes from person to person.

There are similarities at a deeper level, as well. A biological virus is not a living thing. A virus is a fragment of DNA inside a protective jacket. Unlike a cell, a virus has no way to do anything or to reproduce by itself - it is not alive. Instead, a biological virus must inject its DNA into a cell. The viral DNA then uses the cell's existing machinery to reproduce itself. In some cases, the cell fills with new viral particles until it bursts, releasing the virus. In other cases, the new virus particles bud off the cell one at a time, and the cell remains alive.

A computer virus shares some of these traits. A computer virus must piggyback on top of some other program or document in order to get executed. Once it is running, it is then able to infect other programs or documents. Obviously, the analogy between computer and biological viruses stretches things a bit, but there are enough similarities that the name sticks.

What's a "Worm?" - A worm is a computer program that has the ability to copy itself from machine to machine. Worms normally move around and infect other machines through computer networks. Using a Network, a worm can expand from a single copy incredibly quickly. For example, the Code Red worm replicated itself over 250,000 times in approximately nine hours on July 19, 2001.

A worm usually exploits some sort of security hole in a piece of software or the operating system. For example, the Slammer worm (which caused mayhem in January 2003) exploited a hole in Microsoft's SQL server. This article offers a fascinating look inside Slammer's tiny (376 byte) program.

Code Red - Worms use up computer time and Network bandwidth when they are replicating, and they often have some sort of evil intent. A worm called Code Red made huge headlines in 2001. Experts predicted that this worm could clog the Internet so effectively that things would completely grind to a halt.

The Code Red worm slowed down Internet traffic when it began to replicate itself, but not nearly as badly as predicted. Each copy of the worm scanned the Internet for Windows NT or Windows 2000 servers that do not have the Microsoft security patch installed. Each time it found an unsecured server, the worm copied itself to that server. The new copy then scanned for other servers to infect. Depending on the number of unsecured servers, a worm could conceivably create hundreds of thousands of copies.

The Code Red worm was designed to do three things:

1. Replicate itself for the first 20 days of each month

2. Replace Web pages on infected servers with a page that declares "Hacked by Chinese"

3. Launch a concerted attack on the White House Web server in an attempt to overwhelm it

The most common version of Code Red is a variation, typically referred to as a mutated strain, of the original Ida Code Red that replicated itself

on July 19, 2001. According to the National Infrastructure Protection Center:

The Ida Code Red Worm, which was first reported by eEye Digital Security, is taking advantage of known vulnerabilities in the Microsoft IIS Internet Server Application Program Interface (ISAPI) service. Un-patched systems are susceptible to a "buffer overflow" in the Idq.dll, which permits the attacker to run embedded code on the affected system. This memory resident worm, once active on a system, first attempts to spread itself by creating a sequence of random IP addresses to infect unprotected Web servers. Each worm thread will then inspect the infected computer's time clock. The NIPC has determined that the trigger time for the DOS execution of the Ida Code Red Worm is at 0:00 hours, GMT on July 20, 2001. This is 8:00 PM, EST.

Upon successful infection, the worm would wait for the appointed hour and connect to the www.whitehouse.gov domain. This attack would consist of the infected systems simultaneously sending 100 connections to port 80 of [the White House site] (198.137.240.91).

The U.S. government changed the IP address of [the site] to circumvent that particular threat from the worm and issued a general warning about the worm, advising users of Windows NT or Windows 2000 Web servers to make sure they have installed the security patch.

For more information on the Code Red worm, check out these links:

1. Windows NT version 4.0 security patch
2. Windows 2000 Professional, Server and Advanced Server security patch
3. Microsoft: Security Bulletin MS01-033

How They Spread - Early viruses were pieces of code attached to a common program like a popular game or a popular word processor. A person might download an infected game from a bulletin board and run it. A virus like this is a small piece of code embedded in a larger, legitimate program. Any virus is designed to run first when the legitimate program gets executed. The virus loads itself into memory

and looks around to see if it can find any other programs on the disk. If it can find one, it modifies it to add the virus's code to the unsuspecting program. Then the virus launches the "real program." The user really has no way to know that the virus ever ran. Unfortunately, the virus has now reproduced itself, so two programs are infected. The next time either of those programs gets executed, they infect other programs, and the cycle continues.

If one of the infected programs is given to another person on a floppy disk, or if it is uploaded to a bulletin board, then other programs get infected. This is how the virus spreads.

The spreading part is the infection phase of the virus. Viruses wouldn't be so violently despised if all they did was replicate themselves. Unfortunately, most viruses also have some sort of destructive attack phase where they do some damage. Some sort of trigger will activate the attack phase, and the virus will then "do something" - anything from printing a silly message on the screen to erasing all of your data. The trigger might be a specific date, or the number of times the virus has been replicated, or something similar.

As virus creators got more sophisticated, they learned new tricks. One important trick was the ability to load viruses into memory so they could keep running in the background as long as the computer remained on. This gave viruses a much more effective way to replicate themselves. Another trick was the ability to infect the boot sector on floppy disks and hard disks. The boot sector is a small program that is the first part of the operating system that the computer loads. The boot sector contains a tiny program that tells the computer how to load the rest of the operating system. By putting its code in the boot sector, a virus can guarantee it gets executed. It can load itself into memory immediately, and it is able to run whenever the computer is on. Boot sector viruses can infect the boot sector of any floppy disk inserted in the machine, and on college campuses where lots of people share machines they spread like wildfire.

In general, both executable and boot sector viruses are not very threatening any more. The first reason for the decline has been the huge size of today's programs. Nearly every program you buy today comes on a compact disc. Compact discs cannot be modified, and that makes viral infection of a CD impossible. The programs are so big that the only easy

way to move them around is to buy the CD. People certainly can't carry applications around on a floppy disk like they did in the 1980s, when floppies full of programs were traded like baseball cards. Boot sector viruses have also declined because operating systems now protect the boot sector.

Both boot sector viruses and executable viruses are still possible, but they are a lot harder now and they don't spread nearly as quickly as they once could. Call it "shrinking habitat," if you want to use a biological analogy. The environment of floppy disks, small programs and weak operating systems made these viruses possible in the 1980s, but huge executables, unchangeable CDs and better operating system safeguards have largely eliminated that environmental niche.

E-mail Viruses - The Melissa virus in March 1999 was spectacular. Melissa spread in Microsoft Word documents sent via e-mail, and it worked like this:

Someone created the virus as a Word document uploaded to an Internet newsgroup. Anyone who downloaded the document and opened it would trigger the virus. The virus would then send the document (and therefore itself) in an e-mail message to the first 50 people in the person's address book. The e-mail message contained a friendly note that included the person's name, so the recipient would open the document thinking it was harmless. The virus would then create 50 new messages from the recipient's machine. As a result, the Melissa virus was the fastest-spreading virus ever seen! As mentioned earlier, it forced a number of large companies to shut down their e-mail systems.

The ILOVEYOU virus, which appeared on May 4, 2000, was even simpler. It contained a piece of code as an attachment. People who double clicked on the attachment allowed the code to execute. The code sent copies of itself to everyone in the victim's address book and then started corrupting files on the victim's machine. This is as simple as a virus can get. It is really more of a Trojan horse distributed by e-mail than it is a virus.

The Melissa virus took advantage of the programming language built into Microsoft Word called VBA, or Visual Basic for Applications. It is a complete programming language and it can be programmed to do

things like modify files and send e-mail messages. It also has a useful but dangerous auto-execute feature. A programmer can insert a program into a document that runs instantly whenever the document is opened. This is how the Melissa virus was programmed. Anyone who opened a document infected with Melissa would immediately activate the virus. It would send the 50 e-mails, and then infect a central file called NORMAL.DOT so that any file saved later would also contain the virus! It created a huge mess. Microsoft applications have a feature called Macro Virus Protection built into them to prevent this sort of thing. With Macro Virus Protection turned on (the default option is ON), the auto-execute feature is disabled. So when a document tries to auto-execute viral code, a dialog pops up warning the user.

Unfortunately, many people don't know what macros or macro viruses are, and when they see the dialog they ignore it, so the virus runs anyway. Many other people turn off the protection mechanism. So the Melissa virus spread despite the safeguards in place to prevent it.

In the case of the ILOVEYOU virus, the whole thing was human-powered. If a person double-clicked on the program that came as an attachment, then the program ran and did its thing. What fueled this virus was the human willingness to double-click on the executable.

Origins - People create viruses. A person has to write the code, test it to make sure it spreads properly and then release the virus. A person also designs the virus's attack phase, whether it's a silly message or destruction of a hard disk. So why do people do it?

There are at least three reasons. The first is the same psychology that drives vandals and arsonists. Why would someone want to bust the window on someone else's car, or spray-paint signs on buildings or burn down a beautiful forest? For some people that seems to be a thrill. If that sort of person happens to know computer programming, then he or she may funnel energy into the creation of destructive viruses.

The second reason has to do with the thrill of watching things blow up. Many people have a fascination with things like explosions and car wrecks. When you were growing up, there was probably a kid in your neighborhood who learned how to make gunpowder and then built bigger and bigger bombs until he either got bored or did some serious

damage to himself. Creating a virus that spreads quickly is a little like that - it creates a bomb inside a computer, and the more computers that get infected the more "fun" the explosion.

The third reason probably involves bragging rights, or the thrill of doing it - sort of like Mount Everest. The mountain is there, so someone is compelled to climb it. If you are a certain type of programmer and you see a security hole that could be exploited, you might simply be compelled to exploit the hole yourself before someone else beats you to it. "Sure, I could TELL someone about the hole. But wouldn't it be better to SHOW them the hole?" That sort of logic leads to many viruses.

Of course, most virus creators seem to miss the point that they cause real damage to real people with their creations. Destroying everything on a person's hard disk is real damage. Forcing the people inside a large company to waste thousands of hours cleaning up after a virus is real damage. Even a silly message is real damage because a person then has to waste time getting rid of it. For this reason, the legal system is getting much harsher in punishing the people who create viruses.

History - Traditional computer viruses were first widely seen in the late 1980s, and they came about because of several factors. The first factor was the spread of personal computers (PCs). Prior to the 1980s, home computers were nearly non-existent or they were toys. Real computers were rare, and they were locked away for use by "experts." During the 1980s, real computers started to spread to businesses and homes because of the popularity of the IBM PC (released in 1982) and the Apple Macintosh (released in 1984). By the late 1980s, PCs were widespread in businesses, homes and college campuses.

The second factor was the use of computer bulletin boards. People could dial up a bulletin board with a modem and download programs of all types. Games were extremely popular, and so were simple word processors, spreadsheets, etc. Bulletin boards led to the precursor of the virus known as the Trojan horse. A Trojan horse is a program that sounds really cool when you read about it. So you download it. When you run the program, however, it does something un-cool, like erasing your disk. So you think you are getting a neat game but it wipes out your system. Trojan horses only hit a small number of people because they are discovered quickly. Either the bulletin board owner would erase the

file from the system or people would send out messages to warn one another.

The third factor that led to the creation of viruses was the floppy disk. In the 1980s, programs were small, and you could fit the operating system, a word processor (plus several other programs) and some documents onto a floppy disk or two. Many computers did not have hard disks, so you would turn on your machine and it would load the operating system and everything else off of the floppy disk.

Viruses took advantage of these three facts to create the first self-replicating programs.

Where did these buggers come from? Why are they after me in the first place? And when will the madness stop? To provide some perspective, I've pieced together a brief history of the computer virus:

1982. Elk Cloner, considered by some to be the first computer virus found "in the wild," spreads via Apple II floppies and displays this message on screens: "It will get on all your disks. It will infiltrate your chips. Yes, it's Cloner!"

1983. USC grad student Fred Cohen uses the term virus to describe a destructive, self-replicating computer program.

1986. Brain, the first IBM PC virus, appears on 360KB floppies. A text file accompanying the virus contains the name and address of its authors, Pakistani brothers Basit and Amjad Farooq Alvi. The brothers mean no harm. As software vendors, they say they're trying to measure the extent of software piracy in their country. But Brain gets loose and starts copying itself to floppies around the world-without causing any damage.

1987. An experimental virus escapes from a computer lab in Israel. Known as Jerusalem, it strikes on Friday the 13th and deletes programs run on that day. "Stoned," a boot-sector virus that displays the message "Your PC is Now Stoned" at start-up but does no damage, starts to spread.

1988. Cornell grad student Robert Morris, Jr. releases the first worm

across the Internet. The worm ultimately shuts down 6000 Unix (news - Web sites) systems and causes from $10 million to $100 million in damage. The Computer Emergency Response Team is created by the Defense Advanced Research Projects Agency, which sponsored the Internet.

1990. The first viruses from Bulgarian virus writer "Dark Avenger" appear. Also in Bulgaria: the first electronic bulletin board for virus writers to swap code. Eastern Europe would soon become a hotbed of malicious coders. Number of known viruses: less than 300

1991. Tequila, the first polymorphic virus to appear in the wild, is unwittingly distributed on shareware disks. Polymorphic viruses change their appearance to thwart antivirus software; by year's end, dozens of polymorphic viruses have appeared.

1992. Michelangelo becomes the first virus to gain widespread media attention. Written to strike on March 6 (the artist's birthday) and overwrite victims' hard drives, Michelangelo affected an estimated 5000 to 10,000 machines-far fewer than predicted.

1994. E-mails warning of the extremely virulent (but fictitious) Good Times virus begin circulating around the Net, the first of many such virus hoaxes to come.

1995-1997. The Concept virus attacks macros in Microsoft Word; it's the first virus that works equally well on both Windows and Macintosh (news - Web sites) operating systems. Number of known viruses by 1997: 10,000+

1998. Hacker group Cult of the Dead Cow releases Back Orifice, a tool kit for building Trojan horse programs that let hackers infect unprotected PCs and control them remotely.

1999. Melissa appears. It is the first virus to use address books on a victim's computer to e-mail itself to other users. It spreads across the globe in a matter of hours.

2000. A massive distributed denial-of-service attack shuts down Amazon, CNN, Yahoo, and other major Web sites for several days. The

LoveLetter virus spreads to millions of machines overnight, stealing user names and passwords from its victims.

2001. The Anna Kournikova virus appears in the form of an e-mail attachment promised to be a photo of the tennis star. Experts believe it's the first successful virus created by "script kiddie" authors, novice programmers who write viruses using tools downloaded from the Net. The Code Red and Nimda viruses hit thousands of machines, causing more than $2 billion in damage. They are some of the first examples of "blended threats," which combine elements of e-mail worms and traditional viruses.

2002. The Klez worm first appears, overwhelming e-mail servers and disabling antivirus programs. A denial of service attack targets the Internet's 13 root servers, responsible for routing all traffic across the Net, though it causes no lasting damage.

2003. The year of the worm. Successive waves of attacks - Slammer, Blaster, and Sobig - pummel in-boxes around the world, clogging e-mail servers, and costing billions of dollars in lost productivity.

2004. 28,327 new known viruses produced this year, more than any year in history. Number of known viruses 12/31/2004: 112,438.

An Ounce of Prevention - You can protect yourself against viruses with a few simple steps:

1. If you are truly worried about traditional (as opposed to e-mail) viruses, you should be running a more secure operating system like UNIX or Mac OS X. You never hear about viruses on these operating systems because the security features keep viruses (and unwanted human visitors) away from your hard disk.

2. If you are using an unsecured operating system, then buying virus protection software is a *necessary* safeguard. Set heuristics on to “high” if possible. Also, be certain to update your virus definitions frequently, set to auto-update if you can. Also, keep up with operating system and other major software security updates.

3. If you simply avoid programs from unknown sources (like the

Internet), and instead stick with commercial software purchased on CDs, you eliminate almost all of the risk from traditional viruses. In addition, you should disable floppy disk booting - most computers now allow you to do this, and that will eliminate the risk of a boot sector virus coming in from a floppy disk accidentally left in the drive.

4. You should make sure that Macro Virus Protection is enabled in all Microsoft applications, and you should NEVER run macros in a document unless you know what they do. There is seldom a good reason to add macros to a document, so avoiding all macros is a great policy.

5. Open the Options dialog from the Tools menu in Microsoft Word and make sure that Macro Virus Protection is enabled.

6. In the case of the ILOVEYOU e-mail virus, the only defense is a personal discipline. You should never double-click on an attachment that contains an executable that arrives as an e-mail attachment. Attachments that come in as Word files (.DOC), spreadsheets (.XLS), images (.GIF and .JPG), etc., are data files and they can do no damage (noting the macro virus problem in Word and Excel documents mentioned above). A file with an extension like EXE, COM or VBS is an executable, and an executable can do any sort of damage it wants. Once you run it, you have given it permission to do anything on your machine. The only defense is to never run executables that arrive via e-mail.

By following these simple steps, you will be much safer from contracting viruses.