

# CHAPTER 17: UNDERSTANDING VIRII

“My computer operating system is so out of date that people don’t even write viruses for it any more.”

– Thomas Sowell

**F**riday the 13th will be very unlucky indeed if *Saturday the 14th* reformats your hard disk. Is your computer running slower and slower and . . . slower? Perhaps it is *Stoned*. At least the old *Eight Tunes* and *Music Bug* had the good taste to serenade their victims when they seized your PC. The National Computer Security Association (NCSA) tracks more than 9,000 viruses, worms, and their variants, with colorful names like *Dark Avenger*, *Fumble*, and *Typo*.

## COMPUTER PROGRAMS

A computer program works something like this recipe, adapted from the famous Nieman-Marcus e-mail hoax:

---

### CHOCOLATE CHIP COOKIES

- Step 1: Blend 2½ c. oatmeal in a blender to a fine powder.
- Step 2: Cream 1 c. butter, 1 c. sugar, and 1 c. brown sugar.
- Step 3: Add 2 eggs and 1 tsp. vanilla; mix together with 2 c. flour, oatmeal, ½ tsp. salt, 1 tsp. baking powder, and 1 tsp. baking soda.
- Step 4: Add 12 oz. chocolate chips, 4 oz. grated chocolate bar, and 1½ cups chopped nuts.
- Step 5: Roll into balls and place 2" apart on a cookie sheet.
- Step 6: Bake for 10 minutes at 375°.

Just as the cook follows each instruction, step-by-step, the computer follows each instruction of a program, line-by-line. Unlike a cook, the computer performs each instruction blindly, without questioning why or if the instruction is reasonable.

## HOW VIRUSES WORK

Now, imagine the fun you could have if you could secretly append one little step to a friend’s recipe:

- 
- Step 5: Roll into balls and place 2" apart on a cookie sheet.
  - Step 6: Bake for 10 minutes at 375°.
  - Step 7: Frost each cookie with ½ Tbsp. horseradish.

Of course, that would only work if your friend blindly followed each instruction, without questioning why or if the instruction is reasonable.

That’s essentially what a computer virus does. It secretly adds its own code into other programs. Technically, it does more than that; a virus replicates itself. Using our Chocolate Chip Cookie analogy, it would be as if using our tainted recipe would automatically add the errant line to all the other cookie recipes in your friend’s cookbook. A computer worm is simply a virus that lacks this ability to copy itself.

When your PC executes the infected program, the virus or worm may damage partition tables, boot sectors, data files, applications, or even the BIOS.

Viruses can be designed to remain dormant for a period or to be triggered by the date, number of replications, or other events specified by its creator. An early virus, *Lehigh 2.0*, waited in **COMMAND.COM** until it had cloned ten times and then it deleted everything on your hard disk. Long dormancy makes tracking the source of the infection difficult and gives the virus time to spread.

Many viruses appear innocuous, delivering prankish messages to unsuspecting users. After 128 reboots, *Bloody!* displays “Bloody! Jun. 4, 1989,” the date of the Tiananmen Square Massacre. Others, known as “Trojan horses,” are intended to produce catastrophic results. *AIDS* and *Chernobyl* overwrite entire files.

## ABOUT THOSE CUTE NAMES

The *Goner* virus has a cute name—or should I say, it has many cute names, because it also goes by *I-Worm*, *Goner*, *Pentagone*, *Goner-A*, and several other colorful cognomina. To bring some order to this chaotic situation, the Computer Antivirus Research Organization (CARO) has created a formal naming convention for viruses that is gaining acceptance. Created by Vesselin Bontchev,

Fridrik Skulason, and Alan Solomon, the CARONaming Convention gives each virus a meaningful name such as:

**W32.Killer.GE.5211.C@mm**

which is of this general form:

W32	.	Killer	.	GE	.	5211	.	C	.	@mm
Prefix		Family		Group		Major Variant		Minor Variant		Suffix

Names generally won't have all these parts, but the parts should be listed in this order. The prefix indicates the vulnerable platform. Here are some prefixes used today:

PREFIX	MEANING
AOL	America Online® Trojan horse
I-Worm	Internet worm
Java	JAVA™ virus
Linux	Linux® virus
Palm	Palm® OS virus
PWSTEAL	Virus steals passwords
Trojan/Troj	Trojan horse
VBS	Visual Basic Script virus
W32	32-bit Windows® virus
W95	Windows® 95 virus
WM	Word macro virus
WNT	32-bit Windows® NT virus
XM	Excel macro virus

This is followed by:

- **Family:** usually an attribute of the code itself. For example, the Goner virus arrives in an attachment called “Gone.Exe.”
- **Group:** a sub-category of Family (this distinction is rarely used).
- **Major Variant:** a number representing the size of file. For example, W32.Killer.4099 is 4,099 bytes long, while a variant, W32.Killer.5026 is 5,026 bytes long.
- **Minor Variant:** a letter, assigned usually in the order the variant was discovered. The Minor Variant is often used instead of the more cumbersome number of the Major Variant.
- **Suffix:** indicate its means of propagation:

SUFFIX	MEANING
@m	A slow mailer, sending one infected message at a time
@mm	A mass mailer, sending a large number of infected messages at a time.

Thus, if we encounter *Homepage* worm, we can tell from its formal name, VBS.WG2.X@mm, that it is a Visual Basic Script, created by Worm Generator 2 software, minor variant X, which spreads via large numbers of e-mails.

## SPREADING VIRUSES

Shared disks, networks, and Internet downloads are common sources of tainted files. Computer games, often shared between users and posted on the Web and electronic bulletin board systems, are the Typhoid Marys of Cyberspace.

Until the summer of 1995, you had to execute an infected program—that is, a file that ended in **.EXE**, **.COM**, **.CMD**, **.BAT**, **.SCR**, **.PIF**, or **.VBS**—to get a virus. Though they could be corrupted by viruses, data files were not contagious. One didn't fear that copying a Lotus® spreadsheet, even from an infected machine, would harm another computer, its programs, or data. Copying an infected program, though, could be disastrous. Thus, in those early days, viruses were seen by some as your reward for stealing software.

## NEW OGRES

In 1995 the rules changed. Instead of infecting executable files, the *Concept* virus hid within macros in Microsoft® Word documents. A macro is a small set of instructions, saved with the document itself, commonly used to automate repetitive tasks. Saving an infected document triggered *Concept*, which then intervened and saved the document as a template, which prevents saving changes when the document was subsequently edited.

*Concept* spread easily, for a Word document appears quite innocuous by itself, or even as an e-mail attachment. Furthermore, its fingerprint can be changed easily, making it difficult to detect. Within a year of its introduction, *Concept* accounted for almost half of all virus infections. To check for the *Concept* virus:

**Step 1:** Open Microsoft® Word.

**Step 2:** From the pull-down menu, select Tools, Macro, Macros.

The presence of unknown macros in this list, particularly those with six-letter names beginning with AAZ, indicates infection. By July 1996, a similar virus, *Laroux*, infected Excel spreadsheets. *Laroux* replicates by attaching a hidden file to newly saved spreadsheets. Variants have been attached to most Microsoft® documents with .DOC, .XLS, .PPT, and .MDB extensions.

## TWO BIG EXCEPTIONS

As a rule, e-Mail does not contain viruses, but there are two big exceptions to that rule: attachments and *Bubbleboy*-class viruses.

### ATTACHMENTS

E-Mail and chat programs—such as instant messaging—can spread viruses through attached documents. On March 26, 1999, *Melissa* ushered in the modern era of viruses. E-mail infected with *Melissa* contained a Microsoft® Word documents much like *Concept*. When opened, it read your address book and sent copies of itself as attachments to e-Mail via Outlook under your name to the first 50 names listed there, with the message:

**Here is that document you asked for  
. . . don't show anyone else ;-)**

The attachment contained links to pornographic Web sites. When the recipient opens the attachment, the virus spreads to everyone in his or her address book, and on and on. *Melissa* spawned many copycats, such as *Prilissa*, a virus that attacks only if the infected attachment is opened on December 25th, VBS/SST, whose attachment purports to display a picture of tennis player Anna Kournikova, and *ExploreZip*, which read each e-Mail message on your system and then replied to each sender, using the same message header, with a message as innocent as it is ungrammatical:

**Hi, (recipient's name), I received  
your e-mail and I shall send you a  
reply, ASAP. Till then take a look  
at the attached zipped docs. Bye.**

When the recipient opened the attachment, the virus spread again, deleting Word and Excel documents from the victim's hard drive.

Worms spread quickly. MessageLabs, a British security firm, tracked 1.8 million infections of the *MyDoom* worm, in 211 countries, within a week of its debut. It estimated that one in twelve e-mails was infected with *MyDoom*.<sup>1</sup>

### INFORM THE SENDER?

When your anti-virus software intercepts an e-mail message with an infected document, you may be tempted either to scream at the sender or (if you have a civil disposition) to politely inform him or her that he or she sent you a virus.

Don't. Most viruses, like *SoBig*, insert random addresses from its victim's address book into the From: line. In other words, the apparent sender did not send you a virus. Someone who knew the apparent sender did.

### BUBBLEBOY

In late 1999, *Bubbleboy* introduced more e-Mail problems. Merely viewing e-Mail containing the *Bubbleboy* virus in Outlook's preview mode triggers an attack, even if the victim doesn't open an attachment. *Bubbleboy* sends an embedded VBScript command that attaches to the Outlook address book and re-mails itself, infecting everyone in your Address Book. It then changes the registered owner of the infected machine to "Bubbleboy" and the organization to "Vandelay Industries," both references to the *Seinfeld* television show.

*Bubbleboy* requires IE 5.0+ with Windows® Scripting Host installed, which is standard on Windows® 98/ME and 2000 and can be added to Windows® 95. What makes *Bubbleboy* notable is not the damage it does, which is minimal, but the fact that it rewrote the rules for e-mail. Now, merely viewing e-mail, under certain conditions, can spread a virus.

## WEB SITES

Can you get a virus simply by viewing a Web site? Historically, exposure was limited to spyware, such as "browser hijackers" that were more of a nuisance than a threat. Usually this is limited to reporting your surfing patterns.

Some spyware is less benign. *Qhosts*, for example, disabled access to certain search engines and then reset your home page to one of its own liking. True viruses, though, were thought impossible, under normal conditions. In 2004, the *Scob* virus opened a new can of worms by exploiting a flaw in Internet Explorer programming. *Scob* infected thousands of legitimate Web sites, whose visitors would run a JavaScript that would, in turn, retrieve a Trojan horse that recorded a person's keystrokes from a Russian Web site.

### TROJAN HORSES

Trojan horses are one of the most serious threats to computer security. Like the Greeks' soldier-filled giant horse given in tribute to Troy in Homer's *Iliad*, a Trojan horse is a malicious program disguised as something else. A Trojan horse can allow unauthorized users to access your machine remotely. They could:

- steal or change passwords;
- delete or modify files;
- monitor and log your keystrokes;
- steal personal data, such as credit card data;
- reconfigure your firewall; or,
- modify privileges on user accounts.

### ANTI-VIRUS SOFTWARE

There are four kinds of anti-viral software: scanners, integrity checkers, disinfectants, and innoculants. Most anti-virus packages incorporate several of these approaches.

Scanners search for signatures of popular viruses. Viruses attach themselves to programs, so an increase in their size is a tip off that a virus is present. Furthermore, each virus leaves a telltale signature of its presence. For example, *Jerusalem-B* adds exactly 1,808 bytes to infected *.COM* and *.EXE* files. Software firms periodically upgrade their antivirals to include signatures of newly discovered strains. Even then, not all viruses leave signatures. *ZeroHunt*, a memory-resident virus, appends itself to stack space in *.COM* files. In this way, the size of the file does not change, rendering scanners helpless.

Integrity checkers, like scanners, detect viruses, but do not look for signatures. Instead, they compare a file's status before use to its status after use, usually through a procedure called "checksum." Discrepancies suggest in-

fection. Programs that change data within executable files or the Registry can trigger false alarms.

It may be possible to remove a virus with so-called "disinfectants." If an infected program cannot be recovered, the disinfectant typically deletes the entire program. The program must then be reinstalled from the original program diskette. Some viruses operate as terminate-and-stay-resident programs (TSRs), making eradication difficult because, hiding in memory, they can reinfect files as quickly as they are disinfecting.

Innoculants are memory-resident TSRs that prevent viruses from entering the system. Innoculants scan all programs before they are executed for signatures and sometimes monitor your system for suspicious activity. Sophisticated viruses utilize self-encryption and random mutation to evade innoculants.

Anti-virus utilities allow you to update your software periodically over the Internet. An anti-virus program that cannot be updated is often worse than nothing, because it gives people a false sense of security. DOS anti-virus packages such as *Vsafe* or *Msave*, which, though adequate in their day, haven't been updated in years.

### HOW BIG A PROBLEM?

Viruses and worms are not limited to personal systems. The media have publicized—some would say sensationalized—reports of viruses found everywhere from Defense Department networks to NASA mainframes. In 1992, the *Michelangelo* virus was a front page frenzy as its trigger date, March 6—Michelangelo's birthday—approached.

How big is the problem? Most suspected viruses turn out to be something else. Still, nearly 63,000 viruses have attacked the Internet, causing an estimated \$65 billion in damage, according to the NCSA. By some estimates, six to ten new viruses are introduced daily. Any one of them can be a killer.

Why so many? Believe it or not, there are kits available on the Internet to help idiots build viruses. Indeed, Jan "OnTheFly" Dewit reportedly created the *AnnaKournakova* virus from such a kit, "Vbs Worms Generator 1.50b."

Before you rush out to join in the mischief, you should know that U.S. law outlaws the intentional, unauthorized transmission of harmful instructions to a computer used in interstate commerce or communications resulting in

loss or damage greater than \$5,000.<sup>2</sup> Some computer crimes can have even greater penalties. While it is true that perpetrators are rarely caught and convicted, the government has successfully prosecuted several high-profile cases.

On November 2, 1988, Robert Tappan Morris, a Cornell University graduate student, made headlines by creating a worm that brought down over 6,000 servers, virtually paralyzing the Internet. Morris received three years probation, a \$10,000 fine, and was sentenced to perform 400 hours of community service.

### MICROSOFT VULNERABILITY

Religious wars erupt from time-to-time in computerland when the subject of viruses arises. “If you only used [Unix®, Linux®, Mac OS® X], you wouldn’t have these problems,” prattle the usual suspects. They are right—to a degree. First, it is true that Unix®, which underlies these systems, is extremely secure.

By default, Windows® comes with several ports open. These ports facilitate features such as instant-messaging, remote access, and so on. Exploiting open ports and programming flaws is the key to many security issues. In contrast, Mac OS® X comes with all ports closed and locked.

- In Windows®, the Administrator (and—therefore, viruses) can access all areas of the operating system. In Mac OS® X, not even an administrator can access the operating system itself.
- Before a program—such as a virus—can install itself on a Macintosh or Linux box, the user must intervene to accept it. In Windows®, it will simply install itself, without actions (or awareness, perhaps) on your part.

Of course the biggest reason why Microsoft products are targeted by virus writers is that, simply, everybody uses them. If I were to create a virus that made a spreadsheet quack like a duck, I would design it for Microsoft® Excel, not Lotus 1-2-3®, to get the most duck for my buck. It doesn’t help that Microsoft has a finely honed reputation for corporate arrogance and questionable business practices in the hacker community.

A 2003 report by Dan Geer and six other computer-security experts argued that the complexity of Microsoft® Windows and its dominance of the desktop made the U.S. vulnerable to cyber attack.<sup>3, 4</sup> “Microsoft’s monopoly

threatens consumers in a number of ways, but it is clear that it is now also a threat to our security, our safety, and even our national security,” according to Ed Black, President and CEO of the Computer & Communications Industry Association.

### WHO IS RESPONSIBLE?

Most people assume that computer viruses are written by Lex Luthor wannabees with evil global ambitions. The reality is even scarier. Let’s examine a few profiles, to see if we can discern a pattern:

- David L. Smith, 30, named his *Melissa* virus after a Florida stripper. The self-described “pill-head”—an allusion to his affinity to painkillers—lived alone. *Melissa*—the virus, not the stripper—caused over \$80 million damage—quite a sum, considering that Smith had previously declared personal bankruptcy. Smith launched *Melissa* by posting an infected Word document on the alt.sex newsgroup.
- Onel A. de Guzman, 22, authored the “I Love You” virus, which caused \$7-10 billion damage. The college drop-out, lived with his sister in the Philippines. One of his rejected thesis proposals was “Email Password Sender Trojan.” In its purpose section, he wrote: “. . . it will be helpful to a lot of people specially Internet users to get Windows passwords such as Internet Accounts to spend more time on Internet without paying.”<sup>5</sup>
- Chen Ing-Hau, 20, a former college student, created the CIH virus (his initials), because he was angry that he, himself, had been a victim of computer viruses, in the course of his extensive pirating of computer games.<sup>6</sup>
- Romanian college student Dan Dumitru Ciobanu, 24, modified MsBlast to create a denial of service attack against his own university. Ciobanu cleverly left his own nickname and home address in the code. In Romania, the penalty for such a crime is fifteen years in a state prison.
- Simon Vallor, 20, from Llandudno, North Wales, distributed his Redesi worm by exploiting the 9/11 attack on America. Masquerading as a patch from Microsoft that would protect against terrorist virus attacks, it reformatted its victims’ hard disks. Vallor’s own hard disk was found to contain child pornography.

- Jeffrey Lee Parson, 18. Described as a “high-tech loner,” the 320-pound Parson lived with his parents and worked the overnight shift as a gas station attendant when his variant of the Blaster worm attacked 48,000 PCs in 2003.<sup>7</sup> At his sentencing, U.S. District Judge Marsha Pechman blamed Parson’s parents. The Internet, according to Judge Pechman, “has created a dark hole, a dungeon if you will, for people who have mental illnesses or people who are lonely. I didn’t see any parent standing there saying, ‘It’s not a healthy thing to lock yourself in a room and create your own reality.’”<sup>8</sup>
- Sven Jaschan, 17, confessed to creating both Sasser and the 28 variants of the Netsky worm. Described as a shy and withdrawn “computer freak,” Jaschan lived with his mother in Waffensen, Germany.<sup>9</sup> His work created global disruptions from British Airways flights to hospitals in Hong Kong.
- An 21-year-old unemployed “self-taught hacker,” created the Agobot Trojan horse and its Phatbot variant.

These are not warped-but-brilliant X-gen Brainiacs leading a high-tech, international guerilla movement against a repressive system. To the contrary, they are usually young men of little ability (and no girl friends). As Parson’s mother said, “My son is not brilliant; he’s not genius. Anyone that has any computer knowledge could have done what Jeff did.”<sup>10</sup>

She was right. It doesn’t take much talent or a huge amount of computer skills to cause a lot of damage. Dan Dumitru Ciobanu reportedly wrote his code in fifteen minutes. After Parson was apprehended, virus expert Nick Fitzgerald said, “It’s kind of embarrassingly simple. I guess we should praise the Lord for stupid people, right?”<sup>11</sup> Maybe not. This particular stupid person brought down thousands of computers with his stunt.

“Teenage boys seated at computers can contaminate everything simply by bringing to bear the intellectual power necessary to read a comic book,” said George Smith, a senior fellow with GlobalSecurity.org.<sup>12</sup> The scary thing is that if losers like these can wreak such havoc, what might terrorists or hostile nations do with formal and sophisticated cyber-warfare facilities?

## VIRUS HOAXES

You may have received e-Mail warnings of “virtually undetectable” viruses spreading through e-mail, such as *Good Times*, shown in Figure 119.

\*\*\*\*\*VIRUS ALERT\*\*\*\*\*

VERY IMPORTANT INFORMATION, PLEASE READ!

There is a virus that is being sent across the Internet. If you receive an e-mail message with the subject line "Good Times", DO NOT read the message. Delete it immediately!

Some miscreant is sending email under the title "Good Times" nationwide, if you get anything like this DON'T DOWNLOAD THE FILE! It has a virus that rewrites your hard drive, obliterating anything on it. Please be careful and forward this e-mail to anyone you care about.

FCC WARNING!!!

GOOD TIMES PLAGUES INTERNET

The Internet has again been plagued by another computer virus. The reason for all the attention is because of the nature of this virus and the potential security risk it makes. Instead of a destructive Trojan virus (like most viruses!), this virus performs a comprehensive search on your computer, looking for valuable information, such as email and login passwords, credit cards, personal info, etc. The virus can copy this information and SEND IT TO UNKNOWN ADDRESSES.

The Good Times virus is virtually undetectable. It is most likely to attack users viewing Java enhanced Web Pages. Researchers at Princeton University have found this virus on a number of World Wide Web pages and fear its spread.

Please pass this on, for we must alert the general public.

Figure 119

It’s a hoax. There is no such virus. It’s a practical joke, written to panic naïve users. Harmless, right?

Wrong. Most hoaxes, like *Good Times*, direct their hapless victims to forward the message to all their friends. These hoaxes grow exponentially, clogging mail servers, annoying users, and generally scaring the daylights out of users who should know better. Some organizations spend more time debunking hoaxes than handling actual viruses.

Novices aren’t the only dupes. In an article on hackers in the *Law Enforcement Bulletin*, the FBI ominously warned of “new, insidious viruses,” such as *Clinton*, which reportedly infected programs but eradicated itself whenever it was unable to decide which one to infect. When they learned that this virus was a hoax, satirizing President Clinton’s reputation for indecision, our hebetudinous G-Men pulled the errant article from their Web site, but not before the magazine had been mailed to 55,000 subscribers.<sup>13</sup>

## HUMAN FACTORS VIRUSES

Some hoaxes actually can damage your PC. Whoa! How is that possible?

These hoaxes, known as Human Factor Viruses, work like this. You get an e-Mail from a friend, who has just discovered that he has been infected. He fears that he has inadvertently infected everyone in his address book—including you. He confesses his carelessness and implores you to search for a file. If you can find it, you, too, have been infected. You must delete the file and forward the instructions to everyone in your own address book.

I just found out about this virus today and I had it in my machine. Sorry! Since you are in my address book, there's a good chance you could also have this virus which is very easy to eradicate... I am very sorry for any inconvenience!


The virus (called jdbgmgr.exe) is not detected by Norton or McAfee Anti-Virus systems. The virus sits quietly for 14 days before damaging your system. It is sent automatically by messenger and by the address book whether or not you send emails to your contacts. Here's how to check for the Virus and get rid of it. YOU MUST DO THIS!

1. Go to START and click on FIND or SEARCH option
2. In the files/folders option, type the name jdbgmgr.exe
3. DO NOT OPEN IT
4. Be sure to search your C: drive and all sub folders and any other drives you may have
5. Click "find now"
6. The virus has a Teddy Bear icon the name jdbgmgr.exe
7. DO NOT OPEN IT
8. Go to "Edit" (on the menu bar) and choose "Select All" to highlight the file without opening it
9. Go to "File" (on the menu bar) and select "Delete"
10. Go to "Recycle Bin" and delete from there also

IF YOU FIND THIS VIRUS, YOU MUST FORWARD THIS WARNING TO EVERYONE IN YOUR ADDRESS BOOK SO THEY CAN ALSO ERADICATE IT FROM THEIR ADDRESS BOOKS:

1. Open a new email message
2. Click the icon of the address book next to the "TO"
3. Highlight every name and Add to "BCC"
4. Copy the message, paste to email and send.

Figure 120

It sounds plausible, so you search for the file, and—sure enough—it's there. Its icon, , is convincingly suspicious. Only one problem. File xyz—jdbgmgr.exe, in Figure 120—is not a virus, but an obscure part of Windows®. You have just corrupted your own PC. Antivirus software can't protect you from gullibility. (In this case, the damage is small; jdbgmgr.exe is the Microsoft Debugger Registrar for Java, which is used only by

Microsoft Visual J++ 1.1 developers. Next time, you won't be so lucky.)

## SIGNS OF A HOAX

As you gain experience, you will be able to spot a virus hoax on its face. Warning signs include:

- urging you to forward the message to others;
- claiming that e-Mail contains viruses;
- asking you to delete files or edit your Registry;
- claiming that commercial antivirus applications cannot stop it;
- making absurd technological claims, couched in techno-babble; or,
- claiming legitimacy from well-known universities or technology firms.

## LEGACY

Like it or not, viruses have completely changed the cyber-landscape. On a person level, they are preventable annoyances that prey on the stupid and the careless. In a larger sense, they exploded the myth of Internet security. Some would even argue that the viruses of the late 1990s laid the foundations for parts of the Patriot Act and the rest of the Big Brother agenda of post-9/11 America.

## VIRUS HOAXES ON THE WEB

Here are some excellent Web sites that address the issue of virus hoaxes. If nothing else, they're fun to read!

### **AFU & Urban Legends Archive**

<http://www.urbanlegends.com/>

### **Datafellows Hoax Warnings**

<http://www.Europe.Datafellows.com/news/hoax.htm>

### **F-Secure**

<http://www.datafellows.com/virus-info/>

### **Hoaxbusters (DoE)**

<http://hoaxbusters.ciac.org/>

### **Hoax Kill**

<http://www.hoaxkill.com/>

### **McAfee Associates Virus Hoax List**

<http://vil.mcafee.com/>

**Urban Legends Reference Pages**

<http://www.snopes.com/>

**VMyths**

<http://www.vmyths.com/>

**NOTES**

1. <http://www.messagelabs.com/news/virusnews/detail/default.asp?contentItemId=735&region=america>
2. 18 U.S.C. §1030(a)(5)(A)
3. The day after his report was released, Geer, who served as chief technology officer for @Stake Inc. in Cambridge, was fired. Apparently, the emperor really is wearing clothes.
4. Geer, Dan; Bace, Rebecca; Guttman, Peter; Metzger, Perry; Pflieger, Charles P.; Quaterman, John S.; Schneirer, Bruce. "CyberInsecurity: The Cost of Monopoly: How the Dominance of Microsoft's Products Poses a Risk to Security," <http://www.cccanet.org/papers/cyberinsecurity.pdf>
5. <http://www.computerbytesman.com/lovebug/thesis.htm>
6. <http://vx.netlux.org/lib/static/vdat/misc0037.htm>
7. [http://story.news.yahoo.com/news?tmpl=story&cid=528&ncid=528&e=6&u=/ap/20030829/ap\\_on\\_hi\\_te/internet\\_attack\\_profile](http://story.news.yahoo.com/news?tmpl=story&cid=528&ncid=528&e=6&u=/ap/20030829/ap_on_hi_te/internet_attack_profile)
8. <http://apnews.excite.com/article/20050129/D87TFOKG0.html>; retrieved January 29, 2005
9. <http://www.themoscowtimes.com/stories/2004/05/11/251.html>
10. <http://apnews.excite.com/article/20030903/d7takgrg0.html>
11. [http://story.news.yahoo.com/news?tmpl=story&cid=528&ncid=528&e=5&u=/ap/20030830/ap\\_on\\_hi\\_te/internet\\_attack](http://story.news.yahoo.com/news?tmpl=story&cid=528&ncid=528&e=5&u=/ap/20030830/ap_on_hi_te/internet_attack)
12. "Virus Era Hits 5-Year Milestone," March 28, 2004, <http://www.wired.com/news/infostructure/0,1377,62809,00.html>
13. Carter, David L., Ph.D. and Andra J. Katz, Ph.D. "Computer Crime: An Emerging Challenge for Law Enforcement," *Law Enforcement Bulletin*, December 1996.