Global Information Assurance Certification Paper

Evolution of the Computer Virus

Rich Kee
Assignment GSEC version 1.4b
November 16, 2002

Abstract

The evolution of the computer virus, as it relates to the MS-DOS/Windows platform over the past fifteen to twenty years, has grown from a simple, sometimes amusing intrusion on a single personal computer to a full-blown, lethal threat to our computers and computer networks worldwide. This dramatic change in such a relatively short time frame is due to several issues. Some of the major contributing factors are: the availability of more powerful, cheaper personal computers with greater capabilities; the introduction of the world-wide web (Internet) to the mass public; and the standardization of several common, widely accepted computer applications (i.e. Microsoft Word, Microsoft Excel, etc.). These standard applications often contained a number of vulnerabilities that were exploited by virus code writers or hackers.

Hackers have used these factors to develop new and more sophisticated computer viruses or computer worms to further exploit computer systems worldwide. As a result, companies can no longer remain re-active and merely respond to a virus threat after it is discovered within their network structure. Now they are forced to become pro-active (or they should have the awareness to further protect their data and become pro-active), if they want to maintain any form of data security within their network structure.

In the Early Years

A computer virus is a program, a piece of executable code, which has the unique ability to replicate itself. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate. They can attach themselves to just about any type of file and are spread as files that are copied and sent from individual to individual.[1]

The term “computer virus” is often used and confused with “computer worm.” The basic difference between the two is that the computer virus typically relies on human intervention to replicate and the computer worm does not. Once the worm gains access to a computer network, its program is designed to seek out other computers (usually with a specific vulnerability to exploit), and replicate itself. As a result of needing little or no human intervention, the worm is able to spread itself very quickly from one network to another. In some cases the computer worm may initially appear as a virus and after it infects a computer

system, it attempts to seek out other specific systems in a network to exploit a specific vulnerability.

Other terms often used within the antivirus community are the “virus hoax” and “virus joke” program. The virus hoax program is just that, a hoax - typically an email message that purports a newly discovered virus that has no cure, and with the sender suggesting that the email be forwarded to everyone to be forewarned. Some of the telltale signs of a virus hoax sent within an email are: a sense of urgency to forward the email to as many people as possible; that the virus is new and does not have a cure or fix for it; and that the initial discovery of the virus was verified by a reliable source of the computer industry, such as IBM or Microsoft. Another strong sign of a virus hoax is its message often contains excess punctuation, upper case and bold text to emphasize the urgency of the receiver to forward the message.

The joke program usually plays some type of animated cartoon or shows colorful graphics when activated by the user. While neither the hoax or the joke program are harmful viruses or worms and cannot replicate themselves, they can create a problem with network bandwidth and resources as they are emailed to others. As virus hoaxes and joke programs can be used to degradate network resources (similar to an actual computer virus), it is good antivirus policy to address virus hoax issues within company standards. It is also good policy to further communicate some of the potential problems encountered with computer viruses and hoaxes, via company newsletters, email broadcasts and other means of mass communication.

The forwarding of virus hoax or virus joke email has the potential to create the same scenario as a computer virus or computer worm. That scenario is one where the virus or worm was designed to use the resources and bandwidth of a company’s network system to the point where some, if not all of the network resources, become so overloaded that they are not able to function normally.

That type of attack is called a DOS, or Denial Of Service. The hackers goal may be to just slow down or shut down the victimized network system, or they might want to further exploit the network system but inserting specific code or script within their virus to plant a “backdoor” program onto a specific server for future use. A “backdoor” program usually allows the hacker to gain control of the infected server via remote access, to further their cause.

Another virus term often used within the antivirus community is the “Trojan horse” or simply “Trojan” virus. A “Trojan” virus refers to the mythological story of a battle between the Greeks and the Trojans, where the Greeks created a huge wooden horse and left it outside the gates of the Trojan fortress, seemingly as a gift. The Trojans took the horse in, only to be later attacked by the Greeks, who were hidden inside the wooden horse. The “Trojan” virus uses a similar concept

as it masquerades as something else (i.e. a game or utility program), then unleashes a process to delete the victim's files or some other malicious deed.

Viruses are found hidden or attached to just about any type of magnetic media, including diskettes, hard drives, CDs and even tapes used for backups. In the earlier years of computer viruses, many of the first viruses went undetected due to several reasons. Many times the virus itself didn't carry a destructive or obvious payload, such as the deletion of files or the appearance of some bogus message on the computer screen. A specific date, time or other trigger device chosen by the virus creator usually triggered the payload of a virus. The payload of a virus is simply a separate process within the virus that can be triggered to function after a set date, time or other criteria. An example of payloads are the deletion of files, insertion or scrambling of text within a document or a message appearing on the computer screen. Another factor that contributed to the lack of virus detection was there were relatively few viruses propagating at that time. Viruses were not a significant widespread threat for computer software companies to justify creating commercially available antivirus programs to be installed and maintained on company computer systems and networks.

As shown in Table 1, the propagation of computer viruses dramatically changed with the advent of email programs within the corporate structure. Once corporate America realized how convenient and necessary an email program was to their daily processes, they wholehearted embraced them. As a result, where viruses were once a minor nuisance, with email programs such as Lotus Notes or Outlook being implemented, newer and more sophisticated viruses were being created and spreading to a much wider audience, and at a more quicker pace.

Initially the success of hackers in spreading their viruses via email programs was largely due to a factor of human nature and the need to share business documents on a regular basis. In either case, whether an employee unwittingly forwarded a business document or some joke via email, it had the same effect of further propagating the virus. In later years, hackers further refined their viruses to replicate themselves automatically, after the document within the email was opened by the victim.

ICSA Labs Virus Prevalence Survey 2001
Where Do They Come From?
Respondents were asked to identify the means of infection for their most recent virus incident, disaster or encounter. In this survey, respondents could indicate more than one avenue of infection, and totals may exceed 100 percent.[2]

Table 1: Sources of infection, 1996 – 2001

Source of Virus	1996	1997	1998	1999	2000	2001
E-mail Attachment	9%	26%	32%	56%	87%	83%
Internet Downloads	10%	16%	9%	11%	1%	13%
Web Browsing		5%	2%	3%	0%	7%
Don't Know	15%	7%	5%	9%	2%	1%
Auto Software Distribution	0%	2%	1%	0%	0%	2%
Other Vector	0%	5%	1%	1%	1%	2%
Diskette: other	21%	27%	21%	9%	2%	1%
Diskette: From Home	36%	42%	36%	25%	4%	0%
Diskette: Sales Demo	11%	8%	4%	2%	0%	0%
Diskette: Wrapped SW	2%	4%	2%	0%	0%	0%
Diskette: LAN mgr/spvr	1%	3%	1%	0%	0%	0%
Diskette: repair/service	3%	3%	3%	2%	0%	0%
Diskette: malicious person	0%	1%	1%	0%	0%	0%
CD: software distribution	0%	1%	2%	0%	1%	0%
Total Respondents						**300**

This data highlight some important trends. At first glance, it is somewhat surprising to see that the e-mail vector decreased slightly after dramatic growth through 2000. However, it must be understood that the month of August gave rise to CodeRed II and September (the month of data collection) gave us Nimda. Both of these viruses could infect through other Internet means than e-mail. One will also note a sharp increase in the vectors of web browsing and Internet downloads. In addition, there has been a continuance of the last two years' sharp decrease in encounters by diskettes.[2]

Most of the media hype and general consensus of computer users worldwide places the beginning of the computer virus evolution in 1986. During that year, the "Brain" virus first appeared that was simple in nature and relatively harmless. Credit for its creation was given to two Pakistani brothers who ran their own software business. The virus was reportedly propagated whenever any foreign customer purchased their software programs on diskettes. The virus basically copied itself to other diskettes and was harmless in that it just contained the brothers' names, addresses and phone numbers as part of a unique advertising program.[3]

Hackers usually attempt to create one or more scenarios whenever they release a virus. They may intend to have the virus infect and destroy data or have the virus invade and steal sensitive data to be sent back to the hacker. The hackers may create a virus just for notoriety or prestige purposes or to cripple or shut down a potential victim's network or website. Some recent extortion attempts by hackers included the theft of thousands of customer records, including social security numbers and credit card numbers. The hacker then demanded money in exchange for the records, otherwise the hacker threatened to release the records to another buyer or place them on the Internet.

The initial types of viruses were designed to be propagated from a single computer to another as most of the data swapped between computers at that time was from one diskette to another. The viruses were typically transferred to the hard drive or memory of a victim's computer whenever the infected diskette was accessed. Most of the time the viruses went undetected as antivirus programs were not readily available nor thought to be necessary. Then the viruses were spread to other diskettes, and eventually other computers, as other diskettes were inserted into the infected victim's computer.

Viruses being created and propagated during the early years were primarily of two types, the boot sector virus and the file infector virus. The boot sector virus infects the boot sector on a diskette by replacing the original boot sector information with its own program. Since information in the boot sector of a disk loads into the computer's memory before any other information, including any antivirus software, makes eradication of the boot sector virus somewhat unconventional and more work-intensive. Typically the virus was removed by first booting up with a known clean boot diskette, then running the antivirus cleanup program from a command line. The file infector type virus attaches itself to, or associates itself with, another file such as a regular program file or it overwrites some of the program code.[4] Typically, file infector viruses can be easily removed using a good antivirus program that has been kept up to date.

As most of the viruses being created during the mid to late 80s were of the boot sector or file infector type, there wasn't much of a market for antivirus vendors as the nature of the viruses being created during that time didn't lend themselves to being able to easily propagate. This scenario started changing, as, in later years, the viruses became more sophisticated, more lethal, easier/faster to replicate and gained worldwide exposure.

Another virus type that began to appear during that time was the parasitic virus. A parasitic virus attaches itself to programs or executables and is ran at the same time as the program itself. This allows the virus to have the same access as the original program and to trigger its payload. One of the first and more infamous parasitic viruses was the "Jerusalem" virus.[5]

Toward the end of the 80s, computer viruses started getting more recognition and hype from the news media and one of the first to gain widespread attention was the "Jerusalem" virus. The "Jerusalem" virus was set to activate every Friday the 13th and it affected both COM and EXE files and deleted any programs ran on that day.[6] Since there was a lot of media attention focused on the "Jerusalem" virus prior to its outbreak, many companies had plenty of time to implement a fix or detect and clean their systems.

One of the first vendors to start releasing an antivirus software program was IBM Corporation. In September of 1989, IBM sent out version 1.0 of the IBM

scanning software, together with a letter telling their customers what it was, and why they were sending it out. [7] Other companies that started recognizing the need for antivirus software and began developing and releasing their own included McAfee, Symantec, Network Associates and Trend Micro.

Eventually some standards were created among antivirus software vendors where the basic procedures were to install the antivirus program and to constantly update the program on a quarterly or monthly basis. These updates were typically files that contained the latest signatures or data strings that identified newer viruses and triggered the antivirus program to detect and clean or delete the virus and/or worm. As the viruses being created and discovered became more frequent, the updates as well, had to be released more frequently. Currently the typical update file for most antivirus programs is released on a weekly (or usually within 24 hours for new, high-risk viruses) basis.

As the computer industry began to standardize on various common applications such as Microsoft Word, Microsoft Excel and others, computer virus creators began to discover new ways to exploit some of the vulnerabilities of these programs and use those weaknesses to create and propagate their viruses. Application programs written and distributed by Microsoft Corporation were the preferred target of virus creators for several reasons. Microsoft's software was widely distributed and generally held the majority of market share for word processing and spreadsheet programs for personal computer systems. Microsoft had developed a reputation for releasing application software (such as MS/Word and MS/Excel), with a number of software programs bugs and/or vulnerabilities. Finally, some of the controversial issues with Microsoft being a market leader in so many areas of computer software and having the perception of dominating and monopolizing the computer software industry, made it a major target for many hackers who were less than enthused with Microsoft's success or market dominance. These issues provided many opportunities for the hackers to create viruses that had the potential to become more widespread and thus more likely to achieve their ultimate goals.

One of the first virus types that exploited the vulnerabilities of Microsoft programs, such as MS/Word, was the macro virus. A macro virus not only replicated itself like other viruses, but it also had an embedded macro, which allowed it to run additional commands automatically. As an example, if a macro virus was written specifically for MS/Word, the end result was that once a Word document was infected with the virus, it would replicate itself and carry out the macro commands to any other Word document opened or created. The macro virus was then easily spread from one user to another as the infected document was sent via email or downloaded through a company network. The "Concept" virus made its appearance in 1995 and was thought to be the first macro virus, specifically written to infect and replicate via MS/Word documents.

Another MS/Word macro virus that had far-reaching results was the "Melissa" virus. It replicated much faster and farther than any other viruses to date, as the "Melissa" virus, in addition to replicating via Word documents as other Word macro viruses, would also search the victim's computer for the MS email program called Outlook. If the Outlook program was found on the victim's computer, the "Melissa" virus would automatically email a copy of itself to any additional email addresses found in the Outlook email address book. This process would usually take place without the victim even being aware of it. The infected email had the additional benefit of being further propagated as it would go out with the victim's return address on it, further guaranteeing that additional victims wouldn't hesitate to open an infected email document from a friend or acquaintance.

The "Melissa" virus was probably the first virus to gain fast, widespread attention from the public and news media because the virus was fast acting and became widespread. The virus action was similar to the action of a computer worm as it could continue to replicate itself without any human intervention. The virus could replicate itself from a single user to as many as fifty additional email addresses found on the victim's computer. Each of these additional email addresses (if found to be using Microsoft Outlook), would further replicate the virus and send out a maximum of fifty more email addresses and the process would repeat itself ad infinitum. This process would cause the virus to replicate among infected systems in exponential proportions.

Enter the Internet

With the introduction of the Internet or World Wide Web, a whole new method of distribution or replication was made available to hackers. While the creation of the Internet was certainly a milestone for computer users worldwide, with the ability to be able to search for any type of data and to provide information to others at any time and any place, it also made it possible for virus creators to share their virus creating abilities and concepts with fellow virus code writers. This new resource added hundreds of thousands of targets as potential victims, as well as new methods to propagate the viruses.

The Internet gave hackers the additional capability of creating viruses, which could be downloaded within innocent programs or files, by unsuspecting users. These downloaded viruses could be anything from innocent "joke" files to computer worms which gave the hacker remote control access to the victim's computer, with the additional capability of being able to steal confidential data files.

An alarming increase in the use of the victim's computer by the hacker, was to gain remote access to it, via a computer virus or worm. At that point the hacker could use the resources of the computer to tie it into a network of other hacked computers for his own use. This type of attack is called a DDOS, or Distributed

Denial Of Service. The hacker attempts to create a scenario to have hundreds, if not thousands of computers (called "zombies") send out an invalid request or other file command to a specific website or IP address at a specific date and time, with the intention of overloading the website's resources and bringing it down. The intended target could be a competitor's website, a government website or other site selected to be taken out of operation by flooding it with bogus requests or commands from the "zombie" computers.

Some of the more recent, notable viruses that followed the DDOS scenario were the "CodeRed" and "Nimda" viruses. The "CodeRed" virus also acted as a worm in that once it was activated on a victim's computer, it would further search the connected network for a specific computer system to exploit.

In the case of the "CodeRed" virus, it first discovered as it attempted to attack and exploit a known vulnerability of the Microsoft IIS (Internet Information Server) system called a buffer overflow. At that point, the worm executed copies of itself (depending upon its version) onto Windows 2000 systems that had the buffer overflow vulnerability, causing a degradation of the Windows 2000 system.[8]

A buffer overflow vulnerability is one of many possible vulnerabilities that may exist on computer systems. All computer systems have a buffer overflow area which is used to temporarily store data until the computer can further process it, as buffers typically hold a set amount of data any additional data is sent to its buffer overflow area. As an example, a computer keyboard usually has a keyboard buffer which temporarily holds any additional keystrokes sent by the user, until the computer has the time to process the additional keystroke commands.

The hacker will attempt to exploit this type of vulnerability by sending out a large amount of invalid data to the intended victim's computer. The victim's computer receives the invalid data, which slows down its operation, as it doesn't know how to process the large amounts of new invalid data.

Most of the vulnerabilities can be resolved (or patched) by system administrators if they remain vigilant and kept up to date on patches or fixes released by the software/hardware manufacturers to close up the vulnerabilities or holes. But the problem is not easily resolved, as there can be hundreds if not thousands of known vulnerabilities (depending on how many different platforms a company uses) and many systems may need to be patched at least several times a year. Multiply those numbers by the number of vulnerable systems and the process can be very time-consuming and on going.

The "CodeRed" virus was a wake-up call for many companies as they needed to detect and remove the virus, but more importantly, since the virus was replicating very quickly, they needed to patch their vulnerable systems before the worm began to shut them down. The virus also exploited another vulnerability in that

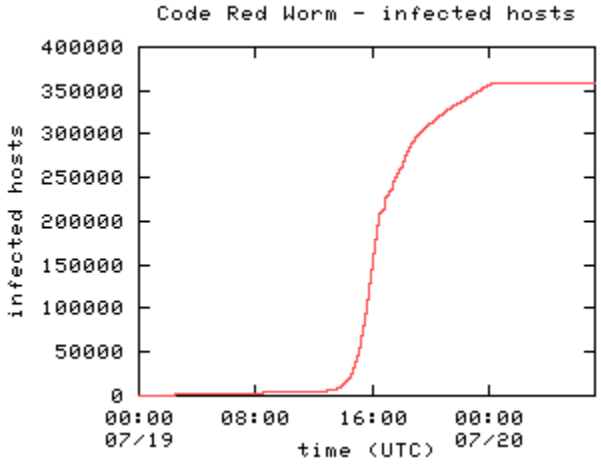
many system administrators were typically overloaded with other work requests, and testing and applying patches was sometimes pushed to a lower priority. That human element factor, along with the process used by “CodeRed” to search for potential vulnerable systems and quickly replicate, resulted in the large number of infected systems as shown in Figure 1. As a single patch can remove or fix several vulnerabilities of a computer system, and as a result of the frantic scramble to apply the patches, many system administrators became more vigilant in keeping their computer system patches properly updated, and later versions of “CodeRed” and other similar worms were not as successful or widespread in exploiting other system vulnerabilities.

"More than 359,000 computers were infected with a version of the Code Red worm in less than 14 hours," said David Moore, SDSC (San Diego Supercomputer Center) senior network researcher and a principal investigator at CAIDA (Cooperative Association for Internet Data Analysis). "At the peak of the infection frenzy, more than 2,000 new hosts were infected each minute."[9]

The Code Red worm infects Web servers by exploiting a security flaw in the Microsoft Internet Information Services (IIS) software package; only systems that run Microsoft software are infected. On July 12, less than a month after the IIS vulnerability was made known to the computer security community, the Code Red worm was detected "in the wild." Once it infects a host, the Code Red worm tries to spread the infection by sending a copy of itself to 99 random IP addresses. Then it waits. On the 20th day of the month, each copy of the worm bombards the White House Web site with messages in an attempt to overload its Web server. Fortunately, the White House Web master was alerted to the problem and changed the numeric IP address of the Web server, which foiled the second phase of the attack.[9]

"We analyzed data from a 24-hour period, beginning midnight UTC July 19, during the critical phase of the infection process," Moore said. "By examining the incoming message traffic to normally unused sections of the Internet we were able to track the spread of the infection as the worm tried to transplant itself to machines at randomly generated addresses on the Net."[9]

Figure 1



This graph shows the rapid spread of the Code Red infestation, from launch of the new variant through cutoff of infection mode. The worm was programmed to switch from an "infection phase" to an "attack phase" at midnight UTC on July 20. The relatively sudden decrease in infection activity appears to be due to this switch.[9]

Another recent prominent virus found in September of 2001 was “Nimda.” It had similar traits as the “CodeRed” virus in that it searched for vulnerabilities on the Microsoft IIS servers. An additional feature of the “Nimda” virus or worm was its ability to modify existing web sites to start offering infected files for download. Also it is the first worm to use normal end user machines to scan for vulnerable web sites. This technique enables Nimda to easily reach Intranet web sites located behind firewalls - something worms such as Code Red couldn't directly do. Nimda uses the Unicode exploit to infect IIS web servers.[10]

Lifecycle of the Nimda virus

The actual lifecycle of Nimda can be split into the following four parts:

1) File infection
Nimda locates EXE files from the local machine and infects them by putting the file inside its body as a resource, thus 'assimilating' that file. These files then spread the infection when people exchange programs such as games.
2) Mass mailer
Nimda locates e-mail addresses via MAPI from your e-mail client as well as searching local HTML files for additional addresses. Then it sends one e-mail to each address. These mails contain an attachment called README.EXE, which might be executed automatically on some systems.
3) Web worm

Nimda starts to scan the Internet, trying to locate www servers. Once a web server is found, the worm tries to infect it by using several known security holes. If this succeeds, the worm will modify random web pages on the site. End result of this modification is that web surfers browsing the site will get automatically infected by the worm.

4) LAN propagation

The worm will search for file shares in the local network, either from file servers or from end user machines. Once found, it will drop a hidden file called RICHED20.DLL to any directory which has DOC and EML files. When other users try to open DOC or EML files from these directories, Word, Wordpad or Outlook will execute RICHED20.DLL causing an infection of the PC. The worm will also infect remote files if it was started on a server.[10]

Summary

Today there are over 50,000 known computer viruses and up to 800 new viruses are discovered each month. More than 50 percent of companies have experienced serious virus disruption.[11] Clearly, computer viruses and worms are here to stay and companies need to become pro-active in maintaining and monitoring an enterprise-wide antivirus program. If a company wants to get serious about protecting their data, it is no longer an option to remain in a re-active mode while trying to stay on top or ahead of today's computer virus threats.

Computer viruses and computer worms have evolved into more sophisticated, lethal threats and by all accounts, will continue to create havoc and widespread damage to potential victims' computer systems. One solution to combat these threats is to implement a multi-layered protection system onto the computer network system. These layers should consist of an antivirus program that is used enterprise-wide throughout the company and a system of checks and balances where the latest software/hardware patches are applied to all of the potential computer systems.

The antivirus program should be loaded, and kept updated, onto all potential computer systems including file servers, email servers, gateways, web servers, as well as individual users' workstations, At a minimum, the antivirus program should have the capability of being able to monitor the status and distribute updates to all critical systems on an enterprise-wide basis, especially for larger networks where many servers and operating system platforms are used.

A system or process should also be in place to patch all affected systems in a timely manner, as needed. For instance, some patches may not be an immediate priority to apply, as they may be a low risk for a vulnerability and can be applied at a later date. But part of the process should require testing the patches before they are applied to the production server, with additional follow-up

communicated to all involved departments, as to the status of the servers to be patched.

Another layer that should be added to any companies' antivirus program is that of antivirus policies and user education. Specific antivirus policies should be created and implemented that convey the company standards for using and maintaining the specific company-approved antivirus program. Users should be made aware of their responsibilities regarding the antivirus program and what procedures are in place for them to follow when needed. User education regarding antivirus procedures needs to be communicated on a frequent on-going basis as the viruses or worms become more prevalent. The education aspect of the antivirus program, as presented to the end users, can be communicated via a company inter-office newsletter or email and for the best effect should be short in length, concise and kept in laymen's' terms.

References

[1]"Virus Primer." 16 Nov. 2002 http://www.trendmicro.com/en/security/general/virus/overview.htm.
[2]Bridwell, Lawrence M. and Peter Tippett, MD, PhD. "ICSA Labs 7th Annual Computer Virus Prevalence Survey 2001." 29 Nov. 2002 www.trendmicro.com/NR/rdonlyres/e5iokdy6cyre4parabrksi4gufe7rs66gqaui7alc6kmfqlzv2adm4pqyz3mf3scepmcz7rv4oayxp/icsavps2001.pdf.
[3]Kazlev, M. Alan. "The Computer Virus – An Incomplete History." 16 Nov. 2002 http://www.kheper.auz.com/resources/computers/security/virus-history.htm.
[4] "Virus Glossary." 16 Nov. 2002 http://www.mcafeeb2b.com/naicommon/avert/avert-research-cventer/virus-glossary.asp.
[5]Theriault, Carole. "An Introduction to Computer Viruses." 17 Nov. 2002 http://www.sophos.com/virusinfo/whitepapers/videmys.html.
[6]"Virus Timeline." 20 Nov. 2002 http://www.infoage.co.nz/virus/timeline.htm.
[7]Solomon, Dr. Alan. "Datacrime (1989)." A Brief History of PC Viruses. 20 Nov. 2002 http://www.bocklabs.wisc.edu/~janda/solomhis.html.
[8]Chien, Eric, and Peter Szor. "Blended Attacks, Exploits, Vulnerabilities and Buffer-Overflow Techniques in Computer Viruses." 20 Nov. 2002 http://securityresponse.symantec.com/avcenter/reference/blended.pdf.
[9]"Network Researchers Track the Worldwide Spread of the "Code Red" Worm." 23 Nov. 2002 http://www.npaci.edu/online/v5.15/codered.html.
[10]"F-Secure Virus Descriptions." 23 Nov. 2002 http://www.europe.f-secure.com/v-descs/nimda.shtml.
[11]Smart, Mike. "Automating AV Enforcement for Small Business." SCMagazine Dec. 2002: 18.