The motivation behind computer viruses

Patrick Carnahan, Dusty Roberts, Zack Shay, Jeff Yeary

Georgia Institute of Technology

Abstract:

Viruses, either helpful or damaging, are conceived by their authors for many differing reasons. Whether for academic reasons, money, fame, protection, or just an attempt to illegally gain access to unauthorized information, all computer viruses bring with them side effects that are typically damaging. By exploring these motivations and studying the impacts of various viruses, it is possible to gain insight into the not so evident reasons for their creation as well as what side effects have occurred as a result of their release.

Introduction

As computers have evolved over time, so has the malicious code designed to attack those computers. Various motivations lie behind malicious code, including educational proofs of concept, fame, money, political statements, spying, and even computer protection. In the early years of the Internet, viruses were written as proof of concept in order to gain fame or further the academic understanding of how they function. It is only in recent years that viruses have been used for spying and making political statements. With the maturation of the Internet and e-commerce, it also did not take long viruses to be written that made money for the author. However, viruses are also being developed, though rarely so, in order to perform beneficial service such as patching holes or shutting down illegal activity.

The first type of virus that will be examined is called a proof of concept virus. This type of virus is often developed early in a product's life. The idea behind this type of virus is to show how a piece of software is vulnerable to unforeseen uses. For example, Microsoft's .NET platform had a proof of concept virus that was written in C# and released before the final version of the platform was authorized by Microsoft to be released (Gold, 2002). Mobile devices, such as cellular phones, handheld organizers, and car computers running Symbian OS, have all been targeted by proof of concept viruses, specifically ones that spread through bluetooth connections.

Proof of concept viruses are usually written by people who consider themselves amateur security researchers. As stated earlier, they are often the first to write a virus for a new system. These amateur researchers normally do not release these viruses into the wild; instead, they discuss their discovery through the use of Internet forums or mailing

lists that are dedicated to writing viruses. Unfortunately there are times when a proof of concept virus gets into the hands of someone who has malicious intent. When this occurs, the virus often spreads quickly and infects many systems.

Writers of proof of concept viruses often claim they write them for academic pursuit. One of the best-known groups for writing these viruses is an international group called 29a Labs. This group explicitly states that they write viruses for the "academic pursuit of new operating systems [and] techniques, [as well as] to invent new technologies" (Policies and Goals). In the same mission statement, 29A Labs claims no responsibility for any consequences resulting from others who may distribute their viruses. They also state that it is their mission to keep wide spread infection to a minimum. Interestingly, they do not restrict their members from delivering destructive payloads, nor do they restrict their members from spreading viruses.

Another type of virus writer includes a diverse group of programmers who write the viruses for fame. These particular virus writers are often placed in a "cyber-terrorism" group because their viruses are written to spread quickly and noticeably. Often when one of these viruses is employed, a window will pop up telling a user that he has run a virus and this pop up will display the alias of the author. These viruses vary in their payload. Some simply spread rapidly and do no damage while others may quickly render a computer system completely useless.

One author, Clinton Haines, better known as Harry McBungus, became very famous on the virus-writing scene in the early to mid 1990s for such viruses as *Terminator-Z*, *TaLoN*, and *NoFrills*. In an interview by Crypt Newsletter in 1995 with this teenage virus writer, the author describes Haines reaction upon hearing that another

NoFrills virus attack has been reported: "[I feel] a surge of delight that it's still out there working its magic and hasn't been retired to a virus museum or old folk's home" (Young, 1995). This virus became infamous in Australia after forcing Australian Telecom to rebuild 1000 computers on their Novell network. This was one year after the financial institution SunCorp was rendered inoperable for 2 days while over 100 workstations and 12 servers were in quarantine being repaired due to an attack of this same virus.

A psychologist named Sarah Gordon, who has studied virus writers for the White House's Cyber Incident Steering Group, did an interview with the BBC explaining the psychology of a virus writer. She claims that some virus writers seek peer approval, which is often gained by seeing their "names in lights". Of course these names are not normally their real names, only the aliases by which they are known on the Internet. Gordon also says that notoriety is only a minor reason people write viruses. She states that most viruses are written because the author does not understand the tremendous consequences that their actions could have upon the computer industry, but instead perceive their creation of new and better viruses to be a competition with other virus authors.

As the use of the Internet began to grow in the late 1980s and early 1990s, viruses began to be created for different reasons. Although a lot of viruses are written for fame and proof of concept, more viruses began to be created for spying on other people, other companies, and other governments. The term spying does not just refer to spyware, which is a form of malicious code that tracks the actions of users and then sells this information to advertisers. Instead, spying viruses refer to any type of virus that is installed on a computer to allow remote access to a computer by unauthorized persons.

These viruses can be in the form of a Trojan horse that creates a backdoor, a virus that installs a key logger for capturing data, or any other type of software that provides unauthorized access to information on a computer system.

Many people, including spammers, governments, and identity thieves, write viruses that harvest or allow unauthorized access to information. These virus writers are often hackers known as "Black Hatters". "Black hatters […] are frequently malicious, unleashing dangerous viruses, crashing servers, defacing web pages, and even waging information warfare financed by business competitors and foreign governments" (Powers, 1997). This type of virus writing can be a very lucrative business. Viruses that steal password lists can be sold to competing companies or governments for access to computer systems. Email addresses harvested by these viruses can be sold to people who send unsolicited emails.

Another common virus type is one that seeks to make a political statement. This statement may include anything from attacking a government website to attacking a corporation. Typically a virus written as a political statement against a company or corporation is written to replicate very quickly but initially remains dormant on the infected machines. At a predetermined date, the virus will begin performing a massively distributed attack on the website of the organization. These attacks are usually in the form of Denial of Service, in which a website is so overwhelmed by requests that it cannot deliver any content to anyone including legitimate customers. Additionally, Denial of Service is often used to make a social statement regarding society's obsession with sex and the media. This can include a virus that exploits the curiosity of people using pornographic or unauthorized celebrity pictures.

At times these viruses do no real harm to the computer system. They simply increase network traffic. Instead of damaging the system they display on the user's screen a message that is of a political nature, such as "Long Live Great SERBIA" (Softpedia, 2005). Others will display a message and at a later date attack the website associated with a political enemy. United States' government websites were often targets of these attacks after the wars in Afghanistan and Iraq. These types of viruses are often written by people who live in those countries in which the war is occurring and they feel as if they are being oppressed by a foreign government, such as the United States, and they view these viruses as a way to spread their message to others across the world.

Despite their popularity, political viruses do not have much effect, either positive or negative, because the people receiving the messages do not lend much credence to messages that are criminal in origin. Political viruses that become well known and spread their message rapidly only cause strife for the political organization that the virus is credited with. According to Mary Landesman, a writer for about.com, these viruses often have a drawback in that they may discredit the organization whose political views may be associated with the virus and therefore this organization may be seen as supporting the spread of viruses (Landesman).

Often a virus writer can use any combination of the above-mentioned viruses in order to make money for the author or for an organization. In the mid 1990s, the rise of e-commerce sites on the Internet introduced a new opportunity for virus writers. Although malicious code had been used for years to steal information, viruses could now be used to quickly and easily confiscate information, hold entire companies hostage, or harvest any information wanted. Other malicious viruses are known to install a phone

dialer on the user's computer and dial expensive foreign phone numbers or pay-per-use phone numbers such as 1-900 numbers.

All of these types of viruses can be very lucrative for the writer. First, harvesting information can provide someone with passwords, email addresses, credit card numbers, or any other type of information the author would like. Credit card numbers and passwords can immediately provide an author with unauthorized access to financial institutions. They can then transfer funds or purchase goods with the stolen information. Another commonly harvested piece of information is an email address. These email addresses are generally used to send out unsolicited commercial email, or spam. Although only approximately 50 out of every 1,000,000 spam messages sent out are ever responded to, it is an extremely rewarding business (Leydon , 2003). It costs little to no money to send out an email, but a spammer can generate $6,000 or more per week simply by mass mailing spam (Wendland, 2002).

Another popular moneymaking practice for malicious coders is to hold an e-commerce site hostage with a Denial of Service attack. Malicious hackers will write a virus that allows them to control thousands of computers at a time, using them to attack websites if they are not paid a ransom. Many times the attacks are aimed at offshore gambling sites, typically ones that may not have the ability to legally fight back. Hackers will use the computers they control to attack a site until a certain amount of funds are deposited into bank accounts. In some cases, these types of attacks have escalated recently and the amount of extortion money demanded has been known to be as high as $50,000 (Cullingworth, 2004).

The final case explored is the very rare case of a virus attempting to do something beneficial for a computer user. A virus of this nature is designed to benefit the person who installed the virus, benefit a system being disrupted by another virus or attack, or benefit society as a whole. These viruses have been known to patch holes in software, attempt to discover and turn in criminals, and to disable other viruses. Corporations as large as Xerox PARC have done research into legitimate uses of these types of viruses.

John Soch and Jon Hupp of Xerox PARC created a virus for doing distributed computation; unfortunately, the experiment went awry and crashed the servers on which it was running (csrc.nist.gov). Other viruses have been written that search computers for child pornography then attempt to report the owner to the government. Although this virus had good intentions, it still used illegal means to accomplish a goal. *Creeper*, one of the earliest viruses written, was later eliminated by a virus called *Reaper* (History of malware).

The motivation behind these "good" viruses is often self-evident. For example, the virus that searched for child pornography was trying to stop an illegal activity. The Xerox PARC virus was attempting to make complex computations faster by distributing the workload on multiple computers. Often the virus may be trying to correct a wrongdoing, such as plugging vulnerabilities in software or deleting another virus. Even though these viruses have good intentions, they are still illegal and the author can be prosecuted just as if they had written a malicious virus.

Case Studies

The Creeper and Reaper Viruses

In the late 1960s, a division of the American Government known as ARPA (Advanced Research Projects Agency) began to fund numerous research sites across the United States with the hope of developing a widespread computer network. This network, originally named ARPANET, exploded rapidly in size and surpassed the expectations of the designers (A brief history of the internet). Although it was first conceived merely as another means of secure communications, numerous other uses for this large computer network were continuously being discovered. One such widely used idea today is that of distributed computing: "the process of aggregating several computing entities to collaboratively run a single computational task" (Distributed computing). The first real world example of the power of distributed computing was in fact a friendly virus.

In the year 1972, the first distributed computing virus was unleashed upon the ARPANET under the name *Creeper* (Malware history). The virus did not perform any malicious actions such as modifying the file system, nor did it even remain on a single computer for any lengthy amount of time. Written for the then popular operating system Tenex, the virus utilized a system's modem to spread itself to other machines connected to the ARPANET (History of malware - 1970s). The interesting thing about this virus is that once it successfully transferred itself to a remote machine, it would delete itself from the previous host machine. Infection was made evident by the following text: "I'M THE CREEPER : CATCH ME IF YOU CAN" (History of malware - 1970s).

The two designers of *Creeper*, Beranek and Newman, are believed to have gotten the idea from a science fiction novel written in the 1970s by author David Gerrold entitled When Harlie Was One (Malware history). The novel told the story of a computer

program which behaved exactly as *Creeper*, but unintentionally, rather than intentionally, spread itself across the network.

Relatively soon after the widespread infection of *Creeper,* a new virus known as *Reaper* was unleashed into the ARPANET. However, this virus was released by its anonymous writer with positive intentions: to spread across the ARPANET much like *Creeper*, but once there it would seek and destroy any detected copies of the *Creeper* virus on the host machine before propagating to its next "victim". It is not clear whether the *Reaper* virus was a defensive response to *Creeper* or an attempt by the original authors to clean up their own mess created by *Creeper*. One thing that is certain, however, is that both of these viruses had an overall positive impact on the computing industry.

Creeper and *Reaper* were "the first infectious computer program[s] and are actually often thought of as the first network virus[es]" (A brief history of the internet). However, not all of the publicity surrounding these two viruses is negative. They did not harm any of the computers which they infected and were "instrumental in exploring the possibility of making use of idle computational power" for distributed computing (A brief history of the internet).

Welchia Worm

Welchia, a viral worm targeted at machines running un-patched versions of Microsoft Windows, is of the virtuous type. Virtuous viruses are a category in which all viruses attempt to help the infected machine rather than harm it (Worm.win32.welchia). The *Welchia* virus was released in 2003 in two different flavors: *Welchia.a* and *Welchia.b*. *Welchia.a* attempts to rid an infected machine of the *Lovesan* (*MS Blaster)*

virus, while *Welchia.b* attempts to rid the machine of the *MyDoom* virus. In both cases an attempt to download and install a patch from Microsoft to prevent future infection is made.

The *Welchia* virus attacks a victim machine in one of two ways: entry through TCP port 135, which is the result of an RPC DCOM vulnerability, and entry through TCP port 80 in order to attack a known vulnerability in Internet Information Services for Windows (Worm.win32.welchia). Once the worm gains entry to a machine, numerous other actions are taken to protect the host machine from future infection. In addition, the host machine quickly becomes the protector, trying to attack other machines to test for the aforementioned vulnerabilities and spreading the virus to those machines that need to be updated.

Once a machine becomes infected, the virus first scans for possible infections of the *Lovesan* or *MyDoom* viruses, removing them if discovered. Next *Welchia* will check such things as the operating system name, locale, and service pack number. Based on this information, the virus will determine whether or not the host machine requires the RPC or IIS patches. If the machine requires updating, the virus will automatically connect to the Microsoft website and download any necessary patches, install the patches, and then reboot the machine to complete the installation process. *Welchia* also starts an automatic Windows Service on the machine, acting as a harmless FTP server to allow the transfer of necessary files to remote machines (W32.welchia.worm, 2004).

After the host machine is virus free and patched accordingly, the virus begins to perform attacks on other machines. Given a host IP address of A.B.C.D, the virus will first attempt to connect to other machines by using a net mask of A.B.0.0. If this is

unsuccessful then it simply computes random IP addresses to use in this second phase (W32.welchia.worm, 2004). Upon finding a valid IP address, the virus attempts to attack a new victim on ports 80 and 135 by exploiting known vulnerabilities on those ports (W32.welchia.worm, 2004). If attacks are successful it then transfers itself to the new victim, downloads any necessary files from the previous host and repeats the process. Utilizing this method of distributing itself across the network, it behaves like a viral worm but with good rather than malicious intentions.

Although this virus was released with good intentions, it still caused mildly damaging effects. In its attempts to rapidly spread across the Internet and defeat the *Lovesan* and *MyDoom* viruses, it actually "soaked up a lot of network traffic, bringing down Air Canada's ticketing system and caus[ed] CSX Corp's railway signaling system to fail" (The vicious world of viruses and worms). It is also believed that *Welchia* committed two major cyber crimes: unauthorized access and continued unsanctioned access (The vicious world of viruses and worms). Based on this information, one important conclusion may be drawn: even viruses with good intentions may have negative effects, and special care must be taken by virus writers to ensure minimal negative effects from their work.

Zafi Worm

Zafi is a mass-mailing worm that propagates by sending email messages to addresses it finds on the infected machine. The first variant of *Zafi*, *Zafi-A*, was released in April 2004. The motivation for the creation of *Zafi-A* was to make a political statement encouraging Hungarian citizens to embrace nationalism. *Zafi-A* is narrowly targeted so as to reach only Hungarian email addresses. It also has a built in sunset

function that will cause it to cease propagation after April 2004. Additionally, anyone running *Zafi-A* on May 1, 2004 was presented with a message box containing the following statement written in Hungarian:

> "People! Hundreds of thousands, millions of Hungarian people live day to day and die from starvation, thirst and poverty in our country. This is while many villainous MPs make millions, and don't even think about what is happening to us.
>
> Puppets are in control. They increase our salaries while doubling our taxes. They talk about justice while their laws protect criminals. They rather waste money on Formula 1 while homeless people die on the streets every day and patients suffer in hospitals without the proper equipment.
>
> Why - why can nobody see this??? Why isn't there a true Hungarian patriot, who puts solving the severe problems of this country ahead his own benefits!!! It is not enough just to want, to talk, or to give speeches about the good and the nice. There must be action. Something must be done by everybody and for everybody!" (Zafi worm displays political tirade, 2004)

Zafi-A infects a machine by posing as an e-card attachment. As soon as the attachment is run, *Zafi* copies itself into the Windows System32 directory using a random filename. It then adds a registry entry to ensure that it will run at startup. While running, *Zafi* scans local files for email address and attempts to send itself to any Hungarian address it finds. *Zafi* is not without teeth, it attempts to close any security related programs it finds such as software firewalls and virus scanners.

A second variant called *Zafi-B* also carried a political message in Hungarian. Anyone infected with *Zafi-B* was presented with the follow message:

> "We demand that the government accommodates the homeless,
> tightens up the penal code and VOTES FOR THE DEATH PENALTY
> to cut down the increasing crime. Jun. 2004, Pécs (SNAF Team)" (Virus information : w32/zafi-b)

Zafi-B made improvements upon the first version by including a more randomized email message, removing the sunset code and adding the ability to propagate on p2p networks as well as email.

Although this virus may be construed as a peaceful protest, it has caused much in the way of collateral damage by consuming bandwidth and clogging email accounts. When released in June, *Zafi-B* accounted for 30% of all malicious code traveling the Internet (Gaudin, 2004). As of March 2005, *Zafi-B* still accounts for 10% of all malicious code traveling the Internet (Zafi-b worm grabs third-place spot, 2005).

Lion Worm and Cheese Worm

The *Lion* worm is a rather unsophisticated Unix shellscript worm. The first two variations of the *Lion* worm relied on a centralized distribution mechanism that has since been shut down (Vision). The third variation copies the *Ramen* worm's distribution method (SANS Institute - Lion Worm, 2001). The author behind this virus, a Chinese cracker named "Lion", founded a group that supports "the cyber defense of the motherland sovereignty of China". This group claims to have created the virus in protest of the Japanese depiction of the Nanking massacre within their history books. The group, calling itself the cnhonker, had the following to say:

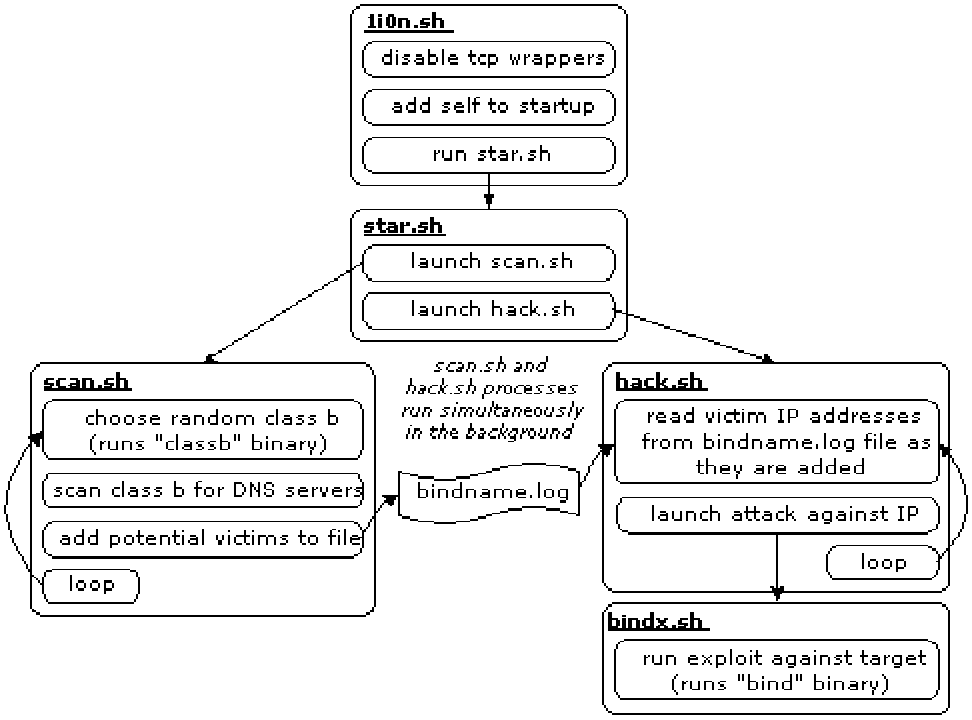
> "because of the Japan's disrespect, cnhonker had been roused,
> and the lion worm is just to tell the Japanese
> Chinese is not sheep, they must be answer for
> They must assume the obligation with their crime
> They must assume their action for the educational book." (Vision)

When asked why they would unleash this worm on the whole Internet and not restrict it to Japanese I.P. addresses they claimed that they could not obtain the correct ranges.

Since this information is readily available and the actual worm itself has no message attached the stated motivations are questionable.

All three versions of the *Lion* worm have a similar modus operandi. "The worm scans random class B address blocks for potential targets. When it finds a responsive name server, the worm launches the BIND exploit against the target. When this exploit is successful, the commands run (via the BIND exploit) cause the new victim to download its own copy of the worm, extract the worm package, and then execute the startup scripts." (Vision)

Figure 1:



(Vision)

The structure of the worm seems to share much of the same code from *ADM*, *Millennium* and *Ramen* worms.

The cnhonker group used this worm to get their name known and then tried to justify their actions with political rhetoric. The overall damage caused by this worm is small when compared to the likes of *Code Red* and *SirCam* which were both released at approximately the same time. *Lion* also managed to spawn another worm known as the *Cheese* worm.

The author of the *Cheese* worm claims to have written it with good intentions. In the code for the *Cheese* worm the author left the following message:

> "removes rootshells running from /etc/inetd.conf
> after a l10n infection... (to stop pesky haqz0rs
> messing up your box even worse than it is already)
> This code was not written with malicious intent.
> Infact, it was written to try and do some good."
> (Net-Worm.Linux.Cheese)

The worm consists of three executables named "cheese", "go" and "psm". "go" is the main entry point and is primarily responsible for executing "cheese". When "cheese" is run it will scan for root shell backdoors and remove them. Then it will generate a new IP address and scan for hosts listening on port 10008. These are usually hosts that have been hacked by *Ramen* or the third variation of *Lion*. Once it finds an infected host it will run a small installation script on the target that downloads a copy of itself.

Although this worm may have been written with good intentions, it manages to eat up resources without really patching the underlying vulnerabilities that allowed *Lion* to infect the machine in the first place. The *Cheese* worm ends up causing almost as much grief as the virus it is intended to stop. It is possible to watch *Lion* infect a whole subnet then watch *Cheese* disinfect it only to have *Lion* come in once again and reinfect the machines behind it.

Aids Information Diskette Trojan

In December 1989, one of the most damaging Trojans ever created was unleashed on the unsuspecting subscribers of *PC Business World* magazine and members of a World Health Organization conference on AIDS. This Trojan, named the *Aids Information Diskette Version 2.0*, was distributed by a company in the United Kingdom by the name PC Cyborg Corporation. Contained along with the 5.25 inch diskette was a very interesting licensing agreement that read:

> "If you install [this] on a microcomputer...then under terms of this license you agree to pay PC Cyborg Corporation in full for the cost of leasing these programs … In the case of your breach of this license agreement, PC Cyborg reserves the right to take legal action necessary to recover any outstanding debts payable to PC Cyborg Corporation and to use program mechanisms to ensure termination of your use... These program mechanisms will adversely affect other program applications... You are hereby advised of the most serious consequences of your failure to abide by the terms of this license agreement; your conscience may haunt you for the rest of your life... and your [PC] will stop functioning normally... You are strictly prohibited from sharing [this product] with others..." (Smith, 2002)

Of course, most receivers of this diskette either did not take the time to read this licensing agreement, or were not even aware that it existed.

Once the Trojan was activated by running the seemingly harmless questionnaire concerning AIDS, the boot file AUTOEXEC.BAT was replaced with a modified version that would track the number of times the machine had been rebooted. Although the number of reboots necessary to activate the Trojan was variable, the approximate number tended toward 90 (Malware history). Upon reaching this reboot limit, the Trojan would proceed to encrypt all files located in the root directory of the hard drive. After the encryption was complete, it would then set the “hidden” attribute on all files, rendering the hard drive completely useless. In order to obtain the encryption key for recovery of

the lost data, the creator required that an amount of $378 be mailed to a post office box located in Panama (Wilding, 1992).

The motivation behind this program is obvious: the creator was attempting to abuse unsuspecting users by blackmailing them into paying him money. However, it is not quite certain whether or not the amount of damage caused by it was anticipated. Since this program was a Trojan and not a virus, automatic replication was not part of the behavior; this malicious program had to be explicitly distributed to and activated by the users of the systems. However, even though this program only infected a small target group of users, irreparable damage was left behind. Approximately 10 years of AIDS research was lost from an organization in Italy due to the panic caused by the installment of the program (Wilding, 1992).

Bibliography:

A brief history of the internet. (n.d.). Retrieved Apr. 10, 2005, from History Web site: http://cse.stanford.edu/class/sophomore-college/projects-01/distributed-computing/html/body_history.html.

Cullingworth, B. (2004). Distributed denial of service attacks no joke. Retrieved Apr. 10, 2005, from Denial of service attacks aimed at blackmailing gambling sites Web site: http://www.winneronline.com/articles/april2004/distributed-denial-of-service-attacks-no-joke.htm.

Distributed computing. (n.d.). Retrieved Apr. 10, 2005, from Distributed computing – Wikipedia, the free encyclopedia Web site: http://en.wikipedia.org/wiki/Distributed_computing.

Gaudin, S. (2004, July 2). Netsky-p and zafi-b worms slug it out for top threat. Datamation, Retrieved Apr 10, 2005, from http://itmanagement.earthweb.com/secu/article.php/3376701.

Gold, S. (2002, Jan 11). First 'proof of concept' .net virus appears. ComputerUser.com, Retrieved Apr 10, 2005, from http://www.computeruser.com/news/02/01/11/news5.html.

Gordon, Sarah. Interview with Stephen Cole. Click Online. BBC. 6 May 2004.

Hayes, B. (2001). The year of the worm . Retrieved Apr. 10, 2005, from SecurityFocus Home Infocus: The Year of the Worm Web site: http://whitehats.com/library/worms/lion/index.html.

History of malware - 1970s. (n.d.). Retrieved Apr. 10, 2005, from Viruslist.com – All About Internet Security Web site: http://www.viruslist.com/en/viruses/encyclopedia?chapter=153310937.

Landesman, M. (n.d.). The politics of viruses. Retrieved Apr. 10, 2005, from The Politics of Viruses Web site: http://antivirus.about.com/library/weekly/aa090902a.htm.

Leydon, John. The Economics of Spam. 18 Nov. 2003. The Register. 9 Apr. 2005 http://www.theregister.co.uk/2003/11/18/the_economics_of_spam/.

Malware history. (n.d.). Retrieved Apr. 10, 2005, from Virus Bulletin : Independent Anti-virus and Anti-spam Advice Web site: http://www.virusbtn.com/resources/malwareDirectory/about/history.xml.

Policies and Goals. 29A Labs. 9 Apr. 2005
http://vx.netlux.org/29a/29a-7/Editorial/29A-7.007.

Political viruses make the rounds more often. 17 Feb. 2005.
Softpedia. 9 Apr. 2005
<http://news.softpedia.com/news/Political-viruses-make-the-rounds-more-often-238.shtml>.

Powers, David. "Hackers Terrorists and Spies." Software
Magazine Oct. 1997. 9 Apr. 2005
http://www.findarticles.com/p/articles/mi_m0SMG/is_n11_v17/ai_20212247.

SANS Institute, (2001). Sans institute - lion worm. Retrieved Apr. 10, 2005, from SANS Institute - Lion Worm Web site: http://www.sans.org/y2k/lion.htm.

Sophos, (n.d.). Virus information: linux/cheese. Retrieved Apr. 10, 2005, from Sophos virus analysis: Linux/Cheese Web site:
http://www.sophos.com/virusinfo/analyses/linuxcheese.html.

Sophos, (2004). Zafi worm displays political tirade. Retrieved Apr. 10, 2005, from Zafi worm displays political tirade Web site:
http://www.sophos.com/virusinfo/articles/zafi.html.

Smith, G. (2002). The original anti-piracy hack. Retrieved Apr. 10, 2005, from SecurityFocus HOME Columnists : The Original Anti-Piracy Hack Web site:
http://www.securityfocus.com/columnists/102.

The vicious world of viruses and worms. (n.d.). Retrieved Apr. 10, 2005, from Recent Viruses and Worms Web site:
http://www.andrew.cmu.edu/user/sylin/67250/overview.html#welchia.

Viruslist.com. Kaspersky Labs. 9 Apr. 2005
http://www.viruslist.com/en/viruses/encyclopedia?chapter=153280553.

Viruslist.com. Kaspersky Labs. 9 Apr. 2005
http://www.viruslist.com/en/viruses/encyclopedia?chapter=153280684.

Viruslist.com, (n.d.). Net-worm.linux.cheese. Retrieved Apr. 10, 2005, from Viruslist.com - Net-Worm.Linux.Cheese Web site:
http://www.viruslist.com/en/viruses/encyclopedia?virusid=23856.

Vision, M. (n.d.). Lion internet worm analysis. Retrieved Apr. 10, 2005, from Whitehats Network Security Resource Web site:
http://whitehats.com/library/worms/lion/index.html.

Wendland, Mike. "Spam king lives large off others' e-mail troubles." Detroit Free Press 22 Nov. 2002. 9 Apr. 2005 http://www.freep.com/money/tech/mwend22_20021122.htm.

Wilding, E. (1992). Popp goes the weasel. *Virus Bulletin*, (1), 2-3.

Worm.win32.welchia. (n.d.). Retrieved Apr. 10, 2005, from Worm.Win32.Welchia Web site: http://www.avp.ch/avpve/worms/win32/welchia.stm.

W32.welchia.worm. (2004). Retrieved Apr. 10, 2005, from Symantec Security Response - W32.Welchia.Worm Web site: http://securityresponse.symantec.com/avcenter/venc/data/w32.welchia.worm.html .

Zafi-b worm grabs third-place spot. (2005). Retrieved Apr. 10, 2005, from Zafi-B Worm Grabs Third-Place Spot Web site: http://www.esecurityplanet.com/alerts/article.php/3487681.

Young, Peter. Famous Australian Virus Writer Dies. Apr. 1995. 9 Apr. 2005 http://www.madchat.org/vxdevl/vdat/misc0006.htm.