10 worst computer viruses of all time

Technology, Computer

10 Worst Computer Viruses of All Time Computer viruses can be a nightmare. Some can wipe out the information on a hard drive, tie up traffic on a computer network for hours, turn an innocent machine into a zombie and replicate and send themselves to other computers. If you've never had a machine fall victim to a computer virus, you may wonder what the fuss is about. But the concern is understandable -- according to Consumer Reports, computer viruses helped contribute to $8. 5 billion in consumer losses in 2008 [source: MarketWatch]. Computer viruses are just one kind of online threat, but they're arguably the best known of the bunch.

Computer viruses have been around for many years. In fact, in 1949, a scientist named John von Neumann theorized that a self-replicated program was possible [source: Krebs]. The computer industry wasn't even a decade old, and already someone had figured out how to throw a monkey wrench into the figurative gears. But it took a few decades before programmers known as hackers began to build computer viruses. While some pranksters created virus-like programs for large computer systems, it was really the introduction of the personal computer that brought computer viruses to the public's attention.

A doctoral student named Fred Cohen was the first to describe self-replicating programs designed to modify computers as viruses. The name has stuck ever since. | Old-school Viruses | | Some of the earliest viruses to infect personal computers included the Apple Viruses, which attacked Apple II computers | | and the Brain virus, which could infect PCs. | In the good old days (i. e. , the early 1980s), viruses depended on humans to do thehard

workof spreading the virus to other computers. A hacker would save the virus to disks and then distribute the disks to other people.

It wasn't until modems became common that virus transmission became a real problem. Today when we think of a computer virus, we usually imagine something that transmits itself via the Internet. It might infect computers through e-mail messages or corrupted Web links. Programs like these can spread much faster than the earliest computer viruses. We're going to take a look at 10 of the worst computer viruses to cripple a computer system. Let's start with the Melissa virus. Worst Computer Virus 10: Melissa In the spring of 1999, a man named David L. Smith created a computer virus based on a Microsoft Word macro.

He built the virus so that it could spread through e-mail messages. Smith named the virus " Melissa," saying that he named it after an exotic dancer from Florida [source: CNN]. [pic] Daniel Hulshizer/AFP/Getty Images A courtroomphotoof David L. Smith, the alleged creator of the Melissa virus. Rather than shaking its moneymaker, the Melissa computer virus tempts recipients into opening a document with an e-mail message like " Here is that document you asked for, don't show it to anybody else. " Once activated, the virus replicates itself and sends itself out to the top 50 people in the recipient's e-mail address book.

The virus spread rapidly after Smith unleashed it on the world. The United States federal government became very interested in Smith's work -- according to statements made by FBI officials to Congress, the Melissa virus " wreaked havoc on government and private sector networks" [source: FBI]. The increase in e-mail traffic forced some companies to discontinue e-mail

programs until the virus was contained. After a lengthy trial process, Smith lost his case and received a 20-month jail sentence. The court also fined Smith $5, 000 and forbade him from accessing computer networks without court authorization [source: BBC].

Ultimately, the Melissa virus didn't cripple the Internet, but it was one of the first computer viruses to get the public's attention. Flavors of Viruses In this article, we'll look at several different kinds of computer viruses. Here's a quick guide to what we'll see: • The general term computer virus usually covers programs that modify how a computer works (including damaging the computer) and can self-replicate. A true computer virus requires a host program to run properly -- Melissa used a Word document. • A worm, on the other hand, doesn't require a host program.

It's an application that can replicate itself and send itself through computer networks. • Trojan horses are programs that claim to do one thing but really do another. Some might damage a victim's hard drive. Others can create a backdoor, allowing a remote user to access the victim's computer system. Next, we'll look at a virus that had a sweet name but a nasty effect on its victims. Worst Computer Virus 9: ILOVEYOU A year after the Melissa virus hit the Internet, a digital menace emerged from the Philippines. Unlike the Melissa virus, this threat came in the form of a worm -- it was a standalone program capable of replicating itself.

It bore the name ILOVEYOU. [pic] Robyn Beck/AFP/Getty Images A screenshot of the ILOVEYOU computer virus The ILOVEYOU virus initially traveled the Internet by e-mail, just like the Melissa virus. The subject of the e-mail said that the message was a love letter from a secret admirer. An

attachment in the e-mail was what caused all the trouble. The original worm had the file name of LOVE-LETTER-FOR-YOU. TXT. vbs. The vbs extension pointed to the language the hacker used to create the worm: Visual Basic Scripting [source: McAfee].

According to anti-virus software producer McAfee, the ILOVEYOU virus had a wide range of attacks: • It copied itself several times and hid the copies in several folders on the victim's hard drive. • It added new files to the victim's registry keys. • It replaced several different kinds of files with copies of itself. • It sent itself through Internet Relay Chat clients as well as e-mail. • It downloaded a file called WIN-BUGSFIX. EXE from the Internet and executed it. Rather than fix bugs, this program was a password-stealing application that e-mailed secret information to the hacker's e-mail address.

Who created the ILOVEYOU virus? Some think it was Onel de Guzman of the Philippines. Filipino authorities investigated de Guzman on charges of theft -- at the time the Philippines had no computer espionage or sabotage laws. Citing a lack of evidence, the Filipino authorities dropped the charges against de Guzman, who would neither confirm nor deny hisresponsibilityfor the virus. According to some estimates, the ILOVEYOU virus caused $10 billion in damages [source: Landler]. Gotcha! As if viruses, worms and Trojan horses weren't enough, we also have to worry about virus hoaxes.

These are fake viruses -- they don't actually cause any harm or replicate themselves. Instead, the creators of these viruses hope that people and media companies treat the hoax as if it were the real deal. Even though these hoaxes aren't immediately dangerous, they are still a problem. Like the boy who cried wolf, hoax viruses can cause people to ignore warnings

about real threats. Now that the love fest is over, let's take a look at one of the most widespread viruses to hit the Web. Worst Computer Virus 8: The Klez Virus [pic] Joe Raedle/Getty Images Fortunately for consumers, there's no shortage of antivirus software suites on the market.

The Klez virus marked a new direction for computer viruses, setting the bar high for those that would follow. It debuted in late 2001, and variations of the virus plagued the Internet for several months. The basic Klez worm infected a victim's computer through an e-mail message, replicated itself and then sent itself to people in the victim's address book. Some variations of the Klez virus carried other harmful programs that could render a victim's computer inoperable. Depending on the version, the Klez virus could act like a normal computer virus, a worm or a Trojan horse.

It could even disable virus-scanning software and pose as a virus-removal tool [source: Symantec]. Shortly after it appeared on the Internet, hackers modified the Klez virus in a way that made it far more effective. Like other viruses, it could comb through a victim's address book and send itself to contacts. But it could also take another name from the contact list and place that address in the " From" field in the e-mail client. It's called spoofing -- the e-mail appears to come from one source when it's really coming from somewhere else. Spoofing an e-mail address accomplishes a couple ofgoals.

For one thing, it doesn't do the recipient of the e-mail any good to block the person in the " From" field, since the e-mails are really coming from someone else. A Klez worm programmed to spam people with multiple e-mails could clog an inbox in short order, because the recipients would be unable to tell what the real source of the problem was. Also, the e-mail's

recipient might recognize the name in the " From" field and therefore be more receptive to opening it. Antivirus Software It's important to have an antivirus program on your computer, and to keep it up to date.

But you shouldn't use more than one suite, as multiple antivirus programs can interfere with one another. Here's a list of some antivirus software suites: • Avast Antivirus • AVG Anti-Virus • Kaspersky Anti-Virus • McAfee VirusScan • Norton AntiVirus Several major computer viruses debuted in 2001. In the next section, we'll take a look at Code Red. Worst Computer Virus 7: Code Red and Code Red II [pic] Chris Hondros/Getty Images The CERT Coordination Center at Carnegie-Mellon university published an advisory alerting the public to the dangers of the Code Red virus. The Code Red and Code Red II worms popped up in the summer of 2001.

Both worms exploited an operating system vulnerability that was found in machines running Windows 2000 and Windows NT. The vulnerability was a buffer overflow problem, which means when a machine running on these operating systems receives more information than its buffers can handle, it starts to overwrite adjacent memory. The original Code Red worm initiated a distributed denial of service (DDoS) attack on the White House. That means all the computers infected with Code Red tried to contact the Web servers at the White House at the same time, overloading the machines.

A Windows 2000 machine infected by the Code Red II worm no longer obeys the owner. That's because the worm creates a backdoor into the computer's operating system, allowing a remote user to access and control the machine. In computing terms, this is a system-level compromise, and it's bad news for the computer's owner. The person behind the virus can access information

from the victim's computer or even use the infected computer to commit crimes. That means the victim not only has to deal with an infected computer, but also may fall under suspicion for crimes he or she didn't commit.

While Windows NT machines were vulnerable to the Code Red worms, the viruses' effect on these machines wasn't as extreme. Web servers running Windows NT might crash more often than normal, but that was about as bad as it got. Compared to the woes experienced by Windows 2000 users, that's not so bad. Microsoft released software patches that addressed the security vulnerability in Windows 2000 and Windows NT. Once patched, the original worms could no longer infect a Windows 2000 machine; however, the patch didn't remove viruses from infected computers -- victims had to do that themselves.

What do I do now? What should you do if you find out your computer has been hit with a computer virus? That depends on the virus. Many antivirus programs are able to remove viruses from an infected system. But if the virus has damaged some of your files or data, you'll need to restore from backups. It's very important to back up your information often. And with viruses like the Code Red worms, it's a good idea to completely reformat the hard drive and start fresh. Some worms allow other malicious software to load onto your machine, and a simple antivirus sweep might not catch them all.

Worst Computer Virus 6: Nimda [pic] SMobile Systems The Symbian Skull Virus affects cell phones, causing them to display a series of skull images like this. Another virus to hit the Internet in 2001 was the Nimda (which is admin

spelled backwards) worm. Nimda spread through the Internet rapidly, becoming the fastest propagating computer virus at that time. In fact, according to TruSecure CTO Peter Tippett, it only took 22 minutes from the moment Nimda hit the Internet to reach the top of the list of reported attacks [source: Anthes]. The Nimda worm's primary targets were Internet servers.

While it could infect a home PC, its real purpose was to bring Internet traffic to a crawl. It could travel through the Internet using multiple methods, including e-mail. This helped spread the virus across multiple servers in record time. The Nimda worm created a backdoor into the victim's operating system. It allowed the person behind the attack to access the same level of functions as whatever account was logged into the machine currently. In other words, if a user with limited privileges activated the worm on a computer, the attacker would also have limited access to the computer's functions.

On the other hand, if the victim was the administrator for the machine, the attacker would have full control. The spread of the Nimda virus caused some network systems to crash as more of the system's resources became fodder for the worm. In effect, the Nimda worm became a distributed denial of service (DDoS) attack. Phoning it In Not all computer viruses focus on computers. Some target other electronic devices. Here's just a small sample of some highly portable viruses: • CommWarrior attacked smartphones running the Symbian operating system (OS). The Skulls Virus also attacked Symbian phones and displayed screens of skulls instead of a home page on the victims' phones. • RavMonE. exe is a virus that could infect iPod MP3 devices made between Sept. 12, 2006, and Oct. 18, 2006. • Fox News

reported in March 2008 that some electronic gadgets leave the factory with viruses pre-installed -- these viruses attack your computer when you sync the device with your machine [source: Fox News]. Next, we'll take a look at a virus that affected major networks, including airline computers and bank ATMs. Worst Computer Virus 5: SQL Slammer/Sapphire pic] Chung Sung-Jun/Getty Images The Slammer virus hit South Korea hard, cutting it off from the Internet and leaving Internet cafes like this one relatively empty. In late January 2003, a new Web server virus spread across the Internet. Many computer networks were unprepared for the attack, and as a result the virus brought down several important systems. The Bank of America's ATM service crashed, the city of Seattle suffered outages in 911 service and Continental Airlines had to cancel several flights due to electronic ticketing and check-in errors.

The culprit was the SQL Slammer virus, also known as Sapphire. By some estimates, the virus caused more than $1 billion in damages before patches and antivirus software caught up to the problem [source: Lemos]. The progress of Slammer's attack is well documented. Only a few minutes after infecting its first Internet server, the Slammer virus was doubling its number of victims every few seconds. Fifteen minutes after its first attack, the Slammer virus infected nearly half of the servers that act as the pillars of the Internet [source: Boutin].

The Slammer virus taught a valuable lesson: It's not enough to make sure you have the latest patches and antivirus software. Hackers will always look for a way to exploit any weakness, particularly if the vulnerability isn't widely known. While it's still important to try and head off viruses before they hit

you, it's also important to have a worst-case-scenario plan to fall back on should disaster strike. A Matter of Timing Some hackers program viruses to sit dormant on a victim's computer only to unleash an attack on a specific date.

Here's a quick sample of some famous viruses that had time triggers: • The Jerusalem virus activated every Friday the 13th to destroy data on the victim computer's hard drive • The Michelangelo virus activated on March 6, 1992 -- Michelangelo was born on March 6, 1475 • The Chernobyl virus activated on April 26, 1999 -- the 13th anniversary of the Chernobyl meltdown disaster • The Nyxem virus delivered its payload on the third of every month, wiping out files on the victim's computer Computer viruses can make a victim feel helpless, vulnerable and despondent.

Next, we'll look at a virus with a name that evokes all three of those feelings. Worst Computer Virus 4: MyDoom [pic] Alex Wong/Getty Images The MyDoom virus inspired politicians like U. S. Senator Chuck Schumer to propose a National Virus Response Center. The MyDoom (or Novarg) virus is another worm that can create a backdoor in the victim computer's operating system. The original MyDoom virus -- there have been several variants -- had two triggers. One trigger caused the virus to begin a denial of service (DoS) attack starting Feb. 1, 2004. The second trigger commanded the virus to stop distributing itself on Feb. 2, 2004. Even after the virus stopped spreading, the backdoors created during the initial infections remained active [source: Symantec]. Later that year, a second outbreak of the MyDoom virus gave several search engine companies grief. Like other viruses, MyDoom searched victim computers for e-mail addresses as part of

its replication process. But it would also send a search request to a search engine and use e-mail addresses found in the search results. Eventually, search engines likeGooglebegan to receive millions of search requests from corrupted computers.

These attacks slowed down search engine services and even caused some to crash [source: Sullivan]. MyDoom spread through e-mail and peer-to-peer networks. According to the security firm MessageLabs, one in every 12 e-mail messages carried the virus at one time [source: BBC]. Like the Klez virus, MyDoom could spoof e-mails so that it became very difficult to track the source of the infection. Oddball Viruses Not all viruses cause severe damage to computers or destroy networks. Some just cause computers to act in odd ways. An early virus called Ping-Pong created a bouncing ball graphic, but didn't seriously damage the infected computer.

There are several joke programs that might make a computer owner think his or her computer is infected, but they're really harmless applications that don't self-replicate. When in doubt, it's best to let an antivirus program remove the application. Next, we'll take a look at a pair of viruses created by the same hacker: the Sasser and Netsky viruses Worst Computer Virus 3: Sasser and Netsky [pic] David Hecker/AFP/Getty Images Sven Jaschan, creator of the Sasser and Netsky viruses, leaves the Verden Court. Sometimes computer virus programmers escape detection.

But once in a while, authorities find a way to track a virus back to its origin. Such was the case with the Sasser and Netsky viruses. A 17-year-old German named Sven Jaschan created the two programs and unleashed them onto the Internet. While the two worms behaved in different ways, similarities in the

code led security experts to believe they both were the work of the same person. The Sasser worm attacked computers through a Microsoft Windows vulnerability. Unlike other worms, it didn't spread through e-mail. Instead, once the virus infected a computer, it looked for other vulnerable systems.

It contacted those systems and instructed them to download the virus. The virus would scan random IP addresses to find potential victims. The virus also altered the victim's operating system in a way that made it difficult to shut down the computer without cutting off power to the system. The Netsky virus moves through e-mails and Windows networks. It spoofs e-mail addresses and propagates through a 22, 016-byte file attachment [source: CERT]. As it spreads, it can cause a denial of service (DoS) attack as systems collapse while trying to handle all the Internet traffic.

At one time, security experts at Sophos believed Netsky and its variants accounted for 25 percent of all computer viruses on the Internet [source: Wagner]. Sven Jaschan spent no time in jail; he received a sentence of one year and nine months of probation. Because he was under 18 at the time of his arrest, he avoided being tried as an adult in German courts. Black Hats Just as you'd find good and bad witches in Oz, you can find good and bad hackers in our world. One common term for a hacker who sets out to create computer viruses or compromise system security is a black hat.

Some hackers attend conventions like the Black Hat conference or Defcon to discuss the impact of black hats and how they use vulnerabilities in computer security systems to commit crimes. So far, most of the viruses we've looked at target PCs running Windows. But Macintosh computers aren't immune to computer virus attacks. In the next section, we'll take a

look at the first virus to commit a Mac attack. Worst Computer Virus 2: Leap-A/Oompa-A [pic] Kevin Mazur Archive 1/WireImage/Getty Images We can thank " Weird Al" Yankovic for warning us of the dreaded " Stinky Cheese" virus.

Maybe you've seen the ad in Apple's Mac computer marketing campaign where Justin " I'm a Mac" Long consoles John " I'm a PC" Hodgman. Hodgman comes down with a virus and points out that there are more than 100, 000 viruses that can strike a computer. Long says that those viruses target PCs, not Mac computers. For the most part, that's true. Mac computers are partially protected from virus attacks because of a concept called security through obscurity. Apple has a reputation for keeping its operating system (OS) and hardware a closed system -- Apple produces both the hardware and the software.

This keeps the OS obscure. Traditionally, Macs have been a distant second to PCs in the home computer market. A hacker who creates a virus for the Mac won't hit as many victims as he or she would with a virus for PCs. But that hasn't stopped at least one Mac hacker. In 2006, the Leap-A virus, also known as Oompa-A, debuted. It uses the iChat instant messaging program to propagate across vulnerable Mac computers. After the virus infects a Mac, it searches through the iChat contacts and sends a message to each person on the list.

The message contains a corrupted file that appears to be an innocent JPEG image. The Leap-A virus doesn't cause much harm to computers, but it does show that even a Mac computer can fall prey to malicious software. As Mac computers become more popular, we'll probably see more hackers create

customized viruses that could damage files on the computer or snarl network traffic. Hodgman's character may yet have his revenge. Breaking into Song While computer viruses can pose a serious threat to computer systems and Internet traffic, sometimes the media overstates the impact of a particular virus.

For example, the Michelangelo virus gained a great deal of media attention, but the actual damage caused by the virus was pretty small. That might have been the inspiration for the song " Virus Alert" by " Weird Al" Yankovic. The song warns listeners of a computer virus called Stinky Cheese that not only wipes out your computer's hard drive, but also forces you to listen to Jethro Tull songs and legally change your name to Reggie. We're down to the end of the list. What computer virus has landed the number one spot? Worst Computer Virus 1: Storm Worm

The latest virus on our list is the dreaded Storm Worm. It was late 2006 when computer security experts first identified the worm. The public began to call the virusthe StormWorm because one of the e-mail messages carrying the virus had as its subject " 230 dead as storm batters Europe. " Antivirus companies call the worm other names. For example, Symantec calls it Peacomm while McAfee refers to it as Nuwar. This might sound confusing, but there's already a 2001 virus called the W32. Storm. Worm. The 2001 virus and the 2006 worm are completely different programs. [pic] Gabriel Bouys/AFP/Getty Images

Professor Adi Shamir of the Weizmann Institute of Sciences in Israel is the leader of the Anti-SpywareCoalition. The Storm Worm is a Trojan horse program. Its payload is another program, though not always the same one.

Some versions of the Storm Worm turn computers into zombies or bots. As computers become infected, they become vulnerable to remote control by the person behind the attack. Some hackers use the Storm Worm to create a botnet and use it to send spam mail across the Internet. Many versions of the Storm Worm fool the victim into downloading the application through fake links to news stories or videos.

The people behind the attacks will often change the subject of the e-mail to reflect current events. For example, just before the 2008 Olympics in Beijing, a new version of the worm appeared in e-mails with subjects like " a new deadly catastrophe in China" or " China's most deadly earthquake. " The e-mail claimed to link to video and news stories related to the subject, but in reality clicking on the link activated a download of the worm to the victim's computer [source: McAfee]. Several news agencies and blogs named the Storm Worm one of the worst virus attacks in years.

By July 2007, an official with the security company Postini claimed that the firm detected more than 200 million e-mails carrying links to the Storm Worm during an attack that pned several days [source: Gaudin]. Fortunately, not every e-mail led to someone downloading the worm. Although the Storm Worm is widespread, it's not the most difficult virus to detect or remove from a computer system. If you keep your antivirus software up to date and remember to use caution when you receive e-mails from unfamiliar people or see strange links, you'll save yourself some major headaches. Malware

Computer viruses are just one kind of malware. Other types include spyware and some kinds of adware. Spyware spies on what a user does with his or her computer. That can include logging keystrokes as a way to discover login

codes and passwords. Adware is a software app that displays ads to users while they use a larger application like a Web browser. Some adware contains code that gives advertisers extensive access to private information. Want to learn more about computer viruses? Take a look at the links on the next page, if you dare. COMPUTER VIRUSES Markus Hanhisalo Department of ComputerScience

Helsinki University ofTechnologyMarkus.fi This report briefly introduces computer viruses and how they effect network security. I have introduced today's virus situation. Many people are afraid of viruses, mostly because they do not know much about them. This report will guide you in the event of a virus infection. Computer viruses and network security is important. There are things that are not public information. Therefore it is good to be a weare of possible network security problems. [pic] Table of Contents 1. Introduction to computer viruses 2. General information about computer viruses . 1 Different Malware types 2. 1. 1 Viruses 2. 1. 2 Trojan 2. 1. 3 Worms 2. 2 Macro viruses 2. 3 Virus sources 2. 3. 1 Why do people write and spread viruses? 2. 4 How viruses act 2. 4. 1 How viruses spread out 2. 4. 2 How viruses activate 2. 5 Viruses in different platforms 2. 5. 1 PC viruses 2. 5. 2 Macintosh viruses 2. 5. 3 Other platforms 3. How to deal with viruses 3. 1 What are the signs of viruses 3. 2 What to do when you find viruses 4. How to protect from viruses 4. 1 How to provide against viruses 4. 2 Different anti-virus programs 5. Computer viruses in Finland 5. A questionnaire survey in Finland about viruses 5. 2 It is going to be a criminal act to make viruses in Finland 6. How computer viruses have spread out around the world 7. Computer viruses and network security 8. Conclusions [pic] 1. Introduction

to Computer Viruses The person might have a computer virus infection when the computer starts acting differently. For instance getting slow or when they turn the computer on, it says that all the data is erased or when they start writing a document, it looks different, some chapters might be missing or something else ubnormal has happened.

The next thing usually the person whose computer might be infected with virus, panics. The person might think that all the work that have been done is missing. That could be true, but in most cases viruses have not done any harm jet, but when one start doing something and are not sure what you do, that might be harmful. When some people try to get rid of viruses they delete files or they might even format the whole hard disk like my cousin did. That is not the best way to act when the person think that he has a virus infection. What people do when they get sick?

They go to see adoctorif they do not know what is wrong with them. It is the same way with viruses, if the person does not know what to do they call someone who knows more about viruses and they get professional help. If the person read email at their PC or if they use diskettes to transfer files between the computer at work and the computer at home, or if they just transfer files between the two computers they have a good possibility to get a virus. They might get viruses also when they download files from any internet site.

There was a time when people were able to be sure that some sites we secure, that those secure sites did not have any virus problems, but nowadays the people can not be sure of anything. There has been viruses even in Microsoft's download sites. In this report I am going to introduce

different malware types and how they spread out and how to deal with them. Most common viruses nowadays are macro viruses and I am going to spend a little more time with them. I am going to give an example of trojan horses stealing passwords. 2. General information about computer viruses 2. 1 Different malware types

Malware is a general name for all programs that are harmful; viruses, trojan, worms and all other similar programs [1]. 2. 1. 1 Viruses A computer virus is a program, a block of executable code, which attach itself to, overwrite or otherwise replace another program in order to reproduce itself without a knowledge of a PC user. There are a couple of different types of computer viruses: boot sector viruses, parasitic viruses, multi-partite viruses, companion viruses, link viruses and macro viruses. These classifications take into account the different ways in which the virus can infect different parts of a system.

The manner in which each of these types operates has one thing in common: any virus has to be executed in order to operate. [2] Most viruses are pretty harmless. The user might not even notice the virus for years. Sometimes viruses might cause random damage to data files and over a long period they might destroy files and disks. Even benign viruses cause damage by occupying disk space and main memory, by using up CPU processing time. There is also the time and expense wasted in detecting and removing viruses. 2. 1. 2 Trojan A Trojan Horse is a program that does something else that the user thought it would do.

It is mostly done to someone on purpose. The Trojan Horses are usually masked so that they look interesting, for example a saxophone. wav file that

interests a person collecting sound samples of instruments. A Trojan Horse differs from a destructive virus in that it doesn't reproduce. There has been a password trojan out in AOL land (the American On Line). Password30 and Pasword50 which some people thought were wav. files, but they were disguised and people did not know that they had the trojan in their systems until they tried to change their passwords. 9] According to an administrator of AOL, the Trojan steals passwords and sends an E-mail to the hackers fake name and then the hacker has your account in his hands. 2. 1. 3 Worms A worm is a program which spreads usually over network connections. Unlike a virus which attach itself to a host program, worms always need a host program to spread. In practice, worms are not normally associated with one person computer systems. They are mostly found in multi-user systems such as Unix environments. A classic example of a worm is Robert Morrisis Internet-worm 1988. [1, 5] [pic] Picture 1 An example of a worm. . 2 Macro virus Macro viruses spread from applications which use macros. The macro viruses which are receiving attention currently are specific to Word 6, WordBasic and Excel. However, many applications, not all of them Windows applications, have potentially damaging and infective macro capabilities too. A CAP macro virus, now widespread, infects macros attached to Word 6. 0 for Windows, Word 6. 0. 1 for Macintosh, Word 6. 0 for Windows NT, and Word for Windows 95 documents. What makes such a virus possible is that the macros are created by WordBASIC and even allows DOS commands to be run.

WordBASIC in a program language which links features used in Word to macros. A virus, named " Concept," has no destructive payload; it merely

spreads, after a document containing the virus is opened. Concept copies itself to other documents when they are saved, without affecting the contents of documents. Since then, however, other macro viruses have been discovered, and some of them contain destructive routines. Microsoft suggests opening files without macros to prevent macro viruses from spreading, unless the user can verify that the macros contained in the document will not cause damage.

This does NOT work for all macro viruses. Why are macro viruses so successful? Today people share so much data, email documents and use the Internet to get programs and documents. Macros are also very easy to write. The problem is also that Word for Windows corrupts macros inadvertently creating new macro viruses. [pic] Picture 2 New macro virus by corruption [12] Corruption's also creates " remnant" macros which are not infectious, but look like viruses and cause false alarms. Known macro virus can get together and create wholly new viruses. [pic]

Picture 3 Macro virus growth, July 1995 to May 1997 [12] There have been viruses since 1986 and macro viruses since 1995. Now about 15 percent of virus are macro viruses. There are about 2. 000 macro viruses and about 11. 000 DOS viruses, but the problem is that macro viruses spreads so fast. New macro viruses are created in the work-place, on a daily basis, on typical end-user machines, not in a virus lab. New macro virus creation is due to corruption, mating, and conversion. Traditional anti-virus programs are also not good at detecting new macro viruses.

Almost all virus detected in the Helsinki University of Technology have been macro viruses, according to Tapio Keihanen, the virus specialist in HUT.

Before macro viruses it was more easy to detect and repair virus infections with anti-virus programs. But now when there are new macro viruses, it is harder to detect macro viruses and people are more in contact with their anti-virus vendor to detect an repair unknown macro viruses, because new macro viruses spread faster than new anti-virus program updates come up. 2. 3 Virus sources Viruses don not just appear, there is always somebody that has made it and they have own reason to so.

Viruses are written everywhere in the world. Now when the information flow in the net and Internet grows, it does not matter where the virus is made. Most of the writers are young men. There are also few university students, professors, computer store managers, writers and even a doctor has written a virus. One thing is common to these writers, all of them are men, women do not waste their time writing viruses. Women are either smarter or they are just so good that never get caught. [1] 2. 3. 1 Why do people write and spread viruses? It is difficult to know why people write them.

Everyone has their own reasons. Some general reasons are to experiment how to write viruses or to test their programming talent. Some people just like to see how the virus spreads and gets famous around the World. The following is a list from news group postings alt. comp. virus and tries to explain why people write and spread viruses. ? they don't understand or prefer not to think about the consequences for other people ? they simply don't care ? they don't consider it to be their problem if someone else is inconvenienced ? hey draw a false distinction between creating/publishing viruses and distributing them ? they consider it to be the responsibility of someone else to protect systems from their creations ? they get a buzz,

acknowledged or otherwise, from vandalism ? they consider they're fighting authority ? they like 'matching wits' with anti virus vendors ? it's a way of getting attention, getting recognition from their peers and their names (or at least that of their virus) in the papers and the Wild List ? they're keeping the anti virus vendors in a job . 4 How viruses act Viruses main mission is to spread out and then get active. Some viruses just spread out and never activate. Viruses when they spread out, they make copies of self and spreading is harmful. 2. 4. 1 How viruses spread out Viruses mission is to hop from program to other and this should happen as quickly as possible. Usually viruses join to the host program in some way. They even write over part of the host program. A computer is infected with a boot sector virus if it is booted from an infected floppy disk. Boot sector infections cannot normally spread across a network.

These viruses spread normally via floppy disks which may come from virtually any source: ? unsolicited demonstration disks ? brand-new software ? disks used on your PC by salesmen or engineers ? repaired hardware A file virus infects other files, when the program to which it is attached is run, and so a file virus can spread across a network and often very quickly. They may be spread from the same sources as boot sector viruses, but also from sources such as Internet FTP sites and newsgroups. Trojan horses spread just like file viruses. A multipartite virus infects boot sectors and files.

Often, an infected file is used to infect the boot sector: thus, this is one case where a boot sector infection could spread across a network. 2. 4. 2 How viruses activate We are always afraid that viruses do something harmful to

files when they get active, but not all the viruses activate. Some viruses just spread out, but when viruses activate they do very different things. Might play a part of melody or playmusicin the background, show a picture or animated picture, show text, format hard disk or do changes to files. As an example, in one unnamed company: over a long period of time, the files in a server were corrupted just a bit.

So backup copies were taken from the corrupted files. And after they noticed that something was wrong, it was too late to get back the data from the backups. That kind of event is the worst that can happen for the uses. There is also talk that viruses have done something to hardware like hard disk or monitor. Viruses can not do any harm to hardware but they can do harm to programs and for example to BIOS so that computer does not start after that. Usually you can start the computer from a boot diskette if the computer does not start otherwise. 2. 5 Viruses in different platforms 2. 5. PC viruses Viruses are mostly written for PC-computers and DOSenvironment. Even though viruses are made for DOS environment, they are working also in Windows, Windows95, Windows NT and OS/2 operating systems. Some viruses like boot sector viruses, do not care what about operating systems. [1] 2. 5. 2 Macintosh viruses Macintosh viruses are not as a big problem as PC viruses are. There are not so many viruses in Macintosh operating system. Macintosh viruses has been found mostly from schools. How many Mac viruses there are? I found out that there are about 2-300 Mac-specific viruses.

There are virtually no macro viruses which have a Mac-specific payload, but all macro viruses can infect on Macs and other platforms which runs Word 6.

x of better. 2. 5. 3 Other platforms Viruses can be found from in almost any kind of computer, such as HP calculators used by students like HP 48- calculators and old computers like Commodore 64 and Unix computers too. [1] In general, there are virtually no non-experimental UNIX viruses. There have been a few Worm incidents, most notably the Morris Worm,. the Internet Worm, of 1988. There are products which scan some Unix systems for PC viruses.

Any machine used as a file server (Novell, Unix etc.) can be scanned for PC viruses by a DOS scanner if it can be mounted as a logical drive on a PC running appropriate network client software such as PC-NFS. Intel-based PCs running Unix e. g. Linux, etc. can also be infected by a DOS boot-sector virus if booted from an infected disk. The same goes for other PC-hosted operating systems such as NetWare. While viruses are not a major risk on Unix platforms, integrity checkers and audit packages are frequently used by system administrators to detect file changes made by other kinds of attack. . How to deal with viruses 3. 1 What are the signs of viruses Almost anything odd a computer may do, can blamed on a computer " virus," especially if no other explanation can readily be found. Many operating systems and programs also do strange things, therefore there is no reason to immediately blame a virus. In most cases, when an anti-virus program is then run, no virus can be found. A computer virus can cause unusual screen displays, or messages - but most don't do that. A virus may slow the operation of the computer - but many times that doesn't happen.

Even longer disk activity, or strange hardware behavior can be caused by legitimate software, harmless " prank" programs, or by hardware faults. A

virus may cause a drive to be accessed unexpectedly and the drive light to go on but legitimate programs can do that also. One usually reliable indicator of a virus infection is a change in the length of executable (*. com/*. exe) files, a change in their content, or a change in their file date/time in the Directory listing. But some viruses don't infect files, and some of those which do can avoid howing changes they've made to files, especially if they're active in RAM. Another common indication of a virus infection is a change to the reassignment of system resources. Unaccounted use of memory or a reduction in the amount normally shown for the system may be significant. In short, observing " something funny" and blaming it on a computer virus is less productive than scanning regularly for potential viruses, and not scanning, because " everything is running OK" is equally inadvisable. 3. 2 What to do when you find viruses First thing what you should do when you find virus is count to ten and stay cool.

You should keep notes on what you do and write down what your virus programs and you computer tells you. If you are not sure what to do, you should call the administrator for future action. In some cases it is not good to start you computer from hard disk, because the virus may active and then do some harm. Second, make sure that you should get sure that it is virus and what virus it is. It is important to know what kind of virus we are dealing with. Companies that make anti-virus programs knows what different viruses does and you can ether call them and ask about that viruses or you can go to their web pages and read about the virus you have.

When you start you computer you should do it from a clean (non-infected) floppy diskette and after that run the virus program. The boot diskette

should be write protected so that virus can not infect the boot diskette too. [6] It is good to take a backup of the file that was infected. Virus program could do some damage to the file and that is why it is good to have a backup. It is good to let you administrator to know about the virus, so viruses would not spread around so much. In TKK PC classes are protected by anti-virus program and that virus program reports to a person, responsible for virus protection. . How to protect from viruses 4. 1 How to provide against viruses Best way to protect yourself is to prepare your computer against viruses in advance. One way to protect you computer is to use updated anti-virus program. When you get an email attachment, you should first check the attachment by checking the file with a anti-virus program. As an example in one unnamed Finnish company all information was mailed in email attachments. There was this one Word document that was mailed to everybody. That email attachment was infected by a macro virus.

Everyone got the infected attachment and those who opened that attachment by Word got that CAP-macro virus. After all there were a few thousand infections. It took lots of time andmoneyto clear that virus. One can protect the computer against boot sector viruses by setting the BIOS to start from a hard disk rather than from a floppy disk. Write protection is a good way to prohibit against viruses. Write protection works well in floppy disks, Windows NT and UNIX, but not that well in Windows and Windows95. 4. Different anti-virus programs There are three different kind of anti-viral packages: activity monitors, authentication or change-detection software, and scanners. Each type has its own strengths and weaknesses. Commercial anti-viral programs have a combination of the above mentioned functions.

[7] There are over ten good anti-viral programs. Most knows programs are Data Fellows F-Prot, EliaShim ViruSafe, ESaSS ThunderBYTE, IBM AntiVirus, McAfee Scan, Microsoft Anti-Virus, Symantec Norton AntiVirus and S&S Dr Solomon's AVTK.

On a day-to-day basis, the average corporation should be very interested in the scan time; these impact strongly the users, who should be scanning hard drives and disks on a daily basis. If a product takes too long to carry out these basic tasks, users will be unwilling to wait, and will stop using it. This is clearly undesirable - the perfect anti-virus product would be one which takes no time to run and finds all viruses. 5. Computer viruses in Finland 5. 1 A questionnaire in Finland about viruses Computer viruses are not uncommon in Finland, especially not in schools and universities. Virus prevention was not well organized in some organizations and tended to be better in government organizations than in local government or in firms" writes Marko Helenius in his Computer viruses in Finland report. He did a large scale questionnaire survey in Finland in the summer 1993. There were not macro viruses at that time yet, so today the virus situation is a bit different, but some results were pretty interesting. The knowledge of viruses was quite poor in all sectors: government, local authorities and companies. Respondents' knowledge of viruses was best in government organizations.

How importance is virus prevention? The most positive attitude to virus prevention was in government organizations. 90% of the government organizations used some kind of anti-virus program, the same in local authority organizations was about 55 % and in companies it was over 60 %. [3] 5. 2 It is going to be a criminal act to make viruses in Finland There is a

new government bill about writing and spreading viruses. If the bill goes through, it is going to be a criminal act to make and spread viruses in Finland and one could get two years in prison or a fine, if one spread or write viruses.

If a person make a virus it would be same thing in court than a person were planning to burn something. It is criminal to make viruses in England, Italy, Netherlands, Switzerland and Russia. It is not punished to make or spread viruses in Finland, according today's penal code. If viruses make harm to somebody that could be punished. Nobody has been punished for that in Finland, even though some Finns has made viruses, for example Finnish Spryer. That virus formatted about 600 hard disks and did lots of damage. They say that it was made in Espoo, but they never got the persons that made that virus.

Virus business in Finland is pretty big. Businesses that have specialized in viruses have about 100 million in sales together. It costs money to stop working and clean up the viruses. Computer viruses put in danger general safety, says Pihlajamaki from Ministry of Justice. It is dangerous if viruses gets to programs that control trains or airplanes. Computer viruses can also be used as a weapon. It is sad that America used computer viruses to slay and to make Iraq's computers non-functional. [4] 6. How computer viruses have spread out around the world Computer viruses are a problem all over the world.

The following picture tells us how many times people have accessed Data Fellows, a company that makes anti-virus program F-Prot, more than 1, 672, 846 per month[10]. It means that people are interesting in virus information. One reason is that people have to deal with viruses. Viruses in not only a

problem in Finland and USA, it is a problem around the world. [pic] Picture 4 Accesses per month Today's most common virus is the macro virus. Cap virus is one of the macro viruses. Last month there were 3100 Cap macro virus accesses during the last 30 days in Data Fellows.

Next common virus was Join the Crew with 1171 accesses and third common was Pen pal Greetings with 895 accesses. [10] [pic] Picture 5 Twenty most accessed virus descriptions during the last 30 days 7. Computer viruses and network security Computer viruses are one network security problem. A few people when asked if computer viruses can cause network security problems answered as follows. Dave Kenney answered from National Computer Security Assoc: " There is one macro virus for MSWord that is received as an attachment to MS Mail messages. If a user has Word open, and double clicks to see the ontents of the attachment, MS Word and the open document is infected. Then the document is mailed to three other users listed in the original user's address book. " " The only information that is leaked is the thing you should be worried about, your password! The trojan sends an E-mail to the hackers fake name and then he has your account at his hands," wrote CJ from American Online. " Rarely, a Word macro virus may accidentally pick up some user information and carry it along; we know of one case where a macro virus " snatched" an innocent user macro that contained a password, and spread it far outside the company where that happened.

In the future, however, it is entirely possible that more network-aware viruses will cause significant network security problems," wrote David Chess from IBM. Marko Helenius wrote from Virus Research Unit, that there has

been some cases when hackers have used trojan horses to gain information. There is one example in one finnish corporation where some money were transferred illegally a year ago. There has been a trojan in the University of Tampere too where the trojan pretend to be a host transfer program. The trojan saved users login name and password to hard disk. 8.

Conclusions There are lots of viruses in the world and new viruses are coming up every day. There are new anti-virus programs and techniques developed too. It is good to be aware of viruses and other malware and it is cheaper to protect you environment from them rather then being sorry. There might be a virus in your computer if it starts acting differently. There is no reason to panic if the computer virus is found. It is good to be a little suspicious of malware when you surf in the Internet and download files. Some files that look interesting might hide a malware.

A computer virus is a program that reproduces itself and its mission is to spread out. Most viruses are harmless and some viruses might cause random damage to data files. A trojan horse is not a virus because it doesn't reproduce. The trojan horses are usually masked so that they look interesting. There are trojan horses that steal passwords and formats hard disks. Marco viruses spread from applications which use macros. Macro viruses spreads fast because people share so much data, email documents and use the Internet to get documents. Macros are also very easy to write.

Some people want to experiment how to write viruses and test their programming talent. At the same time they do not understand about the consequences for other people or they simply do not care. Viruses mission is to hop from program to other and this can happen via floppy disks, Internet

FTP sites, newsgroups and via email attachments. Viruses are mostly written for PC-computers and DOS environments. Viruses are not any more something that just programmers and computer specialist have to deal with. Today everyday users have to deal with viruses.