What are computer viruses and what types of viruses are there

Technology, Computer

Computer Viruses have become a major concern of the government, corporations, and personal computer users. Not only do viruses cause a disturbance to everyday life, they can destroy existing files and can potentially cause major loss to the user. A computer virus is a program that attaches itself to existing files in the computer and infects it. Viruses are named after the biological contagion because a virus attaches itself to healthy files and then spreads to other parts of the computer. This process is replicate of a biological virus that would attach itself to a healthy cell and it spreads to other cells to infect a whole area of the body.

The first acknowledged virus dates back to 1987 called the " Brain". The " Brain" is a boot sector virus. A boot sector virus affects the boot sector which is a small program where information about the drive or disk structure is held. The boot sector is used when the operating system is started up. As a result of the virus attaching itself to the boot sector, every time the computer boots up, the virus is loaded to memory. This type of virus can spread very quickly in environments where computers are shared. A boot sector virus works as long as the computer is on and this guarantees that the virus gets executed because all computers need to boot up.

Other types of viruses are the file or program infector viruses, the macro viruses and most recently, e-mail viruses. The file or program viruses connect themselves to executable programs and then once the programs are run, they load themselves onto memory and from there infect the rest of the computer. Macro viruses attack programs with macros, which are programs that allow users to run a single input and be able to trigger a series of instructions which the computer automatically executes. Macro viruses infect such programs as spreadsheet and word processing files. They are dangerous because once the file is shared the virus is also shared. Also, these viruses can be spread to different platforms such as from Microsoft Windows to Macintosh operating systems which make these viruses more harmful. 1

More recently, e-mail viruses have become popular. Worms such as the " Melissa virus" have been a threat in recent years where the worm would affix itself to a Word Document and then the virus would create an email and send it to the first fifty people of the user's e-mail address book. This caused such a widespread infection that it forced Microsoft and other companies to shut down their email systems for a while. 2 There are also the Trojan viruses that disguise themselves behind something valid and useful and then they would infect files once the disguises are opened. Trojans do not reproduce like worms but it can destroy files and cause harm like them.

History of Viruses

In 1986, the first IBM PC virus called the " Brain" became widespread. Also in 1986, a man named Ralph Burger discovered that he would be able to add code to a DOS executable and that would enable him to replicate files. This was called the " Virdem". Some other notable events that happened in the late 80's to early 90's are the appearance of polymorphic viruses like the " Chameleon", is the appearance of automating production and viral construction sets, CD viruses, and the appearance of the first Windows 95 viruses.

In 1990, the Chameleon virus was created. The Chameleon virus is a benchmark in virus attacks because before these polymorphic viruses, anti-viruses had been using part of virus code to look for viruses. The polymorphic viruses made this method obsolete. These viruses are encrypted so they can hide themselves from the prevention software and therefore can spread throughout the computer without getting noticed. The polymorphic virus is very difficult to detect because every time the virus infects a new file or program, the data on the virus will change its encrypted code. Therefore, even though an antivirus can detect one string of the polymorphic virus, once the virus changes, it will not be effective in preventing another virus attack.

In 1992, the first viral code construction set for IBM PC compatibles was available for purchase. These code construction sets generate viruses at a touch of a button. They include commented source code, object modules and sample infected files. This sets helped construct any type of virus and also help encrypt the code for a deadlier virus package. This made virus creation quick and easy and tempted many programmers to create one just for fun. Other versions of virus construction sets were released later that year such as the Phalcon/ Skism Mass-Produced Code Generator. The later versions of the constructions sets used configurations files which listed all the details of the virus and then formed all the viruses from these files.

In 1994, CD-Rom's were becoming increasingly popular. This caused virus programmers to create viruses that inhabited on CD's. Because many disks are shared, the viruses spread quickly. These viruses are incurable and therefore must be destroyed. There were cases during this year that showed that a virus created on a master copy on a compact disc and then this disk was reproduced in batch sizes and then distributed and infected tens of thousands of systems.

In late 1995 and early 1996, the first Windows95 virus appeared and spread throughout the world. The virus was called the " Win. Tentacle" and it infected hospitals and other institutions in France. 3 Before this, a Window's virus had only been talked about and written about in virus publications and it was a huge event when the first virus became widespread. Since Windows is the most popular and most used operating system, these viruses became more prevalent. Versions of viruses that attack Linux and other operating systems also came about during those years.

More recently in the 21st century, emails and internet are the chosen method of spreading viruses. Such programs as MyDoom and the Melissa virus that attack a person's address book are popular. There are vast amounts of viruses on the loose and many companies and organizations have been trying hard to prevent the damages these viruses can cause.

Anti-viruses

A way to prevent viruses is to use anti-virus software. Anti-viruses fight against virus attacks. First a virus must be reported and then the antivirus software creates a signature file that counteracts the attacking virus. This signature file is then added to an antivirus database and then if the virus attacks again, the system would know how to deal with it. The downside to this method for fighting viruses is that someone must activate the virus first in order for the system to develop a signature file. Another method for identifying viruses is called heuristics. Heuristics tracks all the activity that is running in the computer and then if something is acting like a virus, the system is alerted and the file is either destroyed or quarantined.

The downside of this method is that it is hard to create guidelines that would explain a " virus-like" activity. For example, viruses are known to replicate and if heuristics is used, it can detect the wrong actions and destroy the files when it could be legitimate replication like in program association. Overall, anti-viruses are important to have because they can potentially prevent a harmful virus from destroying valuable information. They, however, are not enough because there are weaknesses within existing methods. There are also so many viruses that are being released that it is hard to keep track of and to prevent all of them. Some popular Anti-virus software that is for sale is the Norton Antivirus, Grisoft, McAfee VirusScan and Panda Titanium Anti-virus.

Why people write viruses

The general public's view of a virus writer is a misconception that he is a " dysfunctional, pasty-faced teenager with no girlfriend and no life". 4 One reason that can be attributed to this generalization is the fact that the internet is able to hide the virus writer's identity so the general public will take on a false impression of the writer. The realistic scenario is that most virus writers are normal people with normal lifestyles and they often do not write codes for malicious purposes.

Virus writers come from different age groups, backgrounds, and countries. Many of them write viruses for different purposes. Most of the teenage virus writers code viruses for the excitement and the challenge that it brings. Additionally, writing a new virus gives the writers credibility and status among their peers. Aside from the benign intentions of teenage virus writers, harm can be caused when they forget to " think about the effect their actions will have on other people". 5 Most virus writers who were teenagers in the past have already grown out of the virus writing phase and consider virus writing an inferior type of coding.

Since the unveiling of the internet to the public, anyone that has access to a computer and internet can now go on the web and search for virus source codes and put together a malicious program and send it off through the internet. Current virus coders who still continue to write viruses and post them (source codes, not executable virus programs) on the internet agree that they " intentionally create and distribute viruses" to harm others. 6 They do note that posting of source codes will not prevent those that have destructive intentions from putting together the source codes into a program and sending it off. The source code writers argue that they should not be held responsible for their creations because the writing of the code does not cause any real harm, but the person who puts them into a program and sends it to others are the culprit. The writing of virus serves many purposes like enhancing a person's knowledge of code and learning how a virus works. Learning about viruses is beneficial because it forces many companies to build better systems to prevent virus attacks.

Another view on virus writers is that they use viruses for harmful intentions. Those that are " motivated by financial gain" are likely to be working with internet companies in order to make a profit off their virus victims. 7 Some of these companies are internet spammers who hire the best virus writers around the world to help them. These virus writers are writing viruses for the sole purpose of stealing personal information from the computers of the people they infect.

There are those virus writers who do it to " claim territory, to make a mark in the internet that will be seen by many others". 8 These types of writers are motivated by the feeling of the global damages they cause by sending their virus through the internet.

Virus writers who write their code to do harm are like other criminals around the world. They have damaging intentions and they should be punished. Those that have outgrown the virus writing phase will eventually be replaced by new virus writers.

Legal Issues

The harm viruses cause to computers is sometimes unquantifiable because it includes economic factors as well as intangible aspects such as reduced consumer confidence. Creating new legislation, however, is a long process and therefore, these crimes face weak laws. For example, the writer of the " I Love You" computer virus had all charges dropped against him in the Philippines even though he released a virus that caused billions of dollars in damages all over the world because there were no laws in place to prosecute him by.

However, in the United States, lawmakers are attempting to keep up with the quick changing technology and the problems that come with it. Although distribution of a virus with a malicious intent is considered a federal crime, the sole act of writing or providing easy access to virus code is not. The United States courts have come to establish original computer code as a form of intellectual property, putting it in the same category as music and artwork. Intellectual property is protected under the 1st Amendment of free speech. This was established in 1995 after a graduate student, Daniel Bernstein, filed a law suit against the government for violating his constitutional right because to post an encryption program, the government ruled that he would need to register as an international weapons dealer fearing that the program would mask illegal activity.

These freedoms of speech associated with intellectual property are restricted if they harm the public's welfare. They, however, are closely guarded by the courts even in instances where it may seem there is potential for harm. " Many potentially dangerous pieces of intellectual property have appeared in the U. S. - articles on how to make bombs and how to commit assassinations-

and the courts have routinely suppressed any restraints on free speech."(cc and 1st amendment)

Another problem arises when trying to define the term 'malicious', a requirement to proceed with federal prosecution of virus distribution, " any code that interferes with the smooth operation of a person's system could conceivably be characterized as malicious." (PC world) Essentially, this means that if a program makes the computer run slower because it takes up a lot of space, even if it helps the user or is something the user voluntarily installed, it could be characterized as 'malicious'. These two issues leave virus writers with a strong argument and a small chance of being convicted or even prosecuted.

The Computer Fraud and Abuse Act (CFAA) has made it illegal to distribute code either with the intention of causing damage or economic loss or doing so recklessly; and has outlined a list of criminal penalties without infringing upon the 1st amendment rights of virus writers. At first when the CFAA was enacted in 1984, it pertained only to government computers or those owned by large corporations. The National Information Infrastructure Protection Act expanded the CFAA in 1996 to include any computer connected to the internet. Exhibit 1 details what the CFAA prohibits.

Some more recent computer viruses are doing more than annoying users, some are being written to access private information, steal money, and even identities. Electronic mail is now being treated as physical mail, unauthorized access to the messages, either through interception or hacking into an account, is considered a federal crime as a result of the Electronic Communications Privacy Act. While ISP employees are allowed to read messages to protect themselves, officials can obtain warrants to access this information and a recently added clause requires that carriers modernize their equipment to make it capable of electronic surveillance. There was a worm written that would take a penny from each wire transfer and deposit it into a bank account, the Wire Fraud Act makes it illegal to use wire communications systems " to commit a fraud to obtain money or property" and makes " computer-aided theft involving the use of interstate wires or mails" a criminal offense.

Finally, identity theft is becoming a bigger problem with the rapid growth of e-commerce. Encryption makes web pages a little more secure, but the uneducated e-commerce consumer sometimes fails to protect his or her information and ends up with a case of stolen identity. The Identity Theft and Assumption Deterrence Act (ITADA) makes the theft of any information that specifically identifies an individual a federal crime and addresses the compensation and relief associated with the damages.

States have also attempted to coin their own laws but they are limited to addressing unauthorized access to networks or sabotage. This is because other computer laws they try to address come up against the roadblock of the extraterritoriality of the crimes. Therefore, the best legislation enacted so far is the CFAA.