A History Of Computer Viruses Essay, Research Paper

Overview

In the following report, computer viruses will be explained in detail. A lengthy and informative description of the evolution and history on microcomputer viruses will be given, to give you a background of their origin for some understanding of how they came to be.

The next segment in the report is on how to combat computer viruses with the development of anti-virus applications.

The current status of microcomputer viruses will also be discussed, naming the most common types of viruses and the most harmful type at this present point in time.

Details of the most recent outbreaks of computer viruses, such as the Melissa , I Love You and the most recent Anna Kournikova viruses will be explained, and why they are so harmful.

I will also give you my recommendations on how to combat this threat of computer viruses, what Anti-virus Applications that I believe should be used, and why updating your virus definitions for these programs on a regular basis is so vital and important in your quest to have a happy and uninfected computer.

And finally, I give you my conclusion in which I can only hope that you will find helpful.

A History Of Computer Viruses

The term Virus was not used to describe a self-replicating computer program until the American electrical engineer named Fred Cohen associated the term with it in 1983.

In the 1950 s at Bell Laboratories, John von Neumann s theory in which he made in 1949 was put to the test. His theory stated that it was (MS Encarta 98, Virus [computer], History) Theoretically possible for a computer program to replicate . His theory was tested after a game called Core Wars was developed whereby (MS Encarta 98, Virus [computer], History) Players created tiny computer programs that attacked, erased, and tried to propagate on an opponent s system .

In the late 1960 s through to the early 1970 s, the program called The Rabbit was constantly appearing on the mainframes at the time. Kaspersky (www.avp.ch) These programs cloned themselves, occupied system resources, thus lowering the productivity of the system . These viruses were only localised, as they did not spread from one system to another and are thought to have only been pranks or mistakes by programmers.

The Univac 1108 and IBM 360/370 systems were infected with one of the first known computer viruses, Pervading Animal . This virus attached itself to executable files, which damaged the infected file.

In 1986 the first stealth virus hit IBM Compatible PC s, called the BRAIN virus. The fact that it was Stealth meant that it was undetectable, and Kaspersky (www.avp.ch) if there was an attempt to read the infected sector, the virus substituted it with a clean original one . It originated in Pakistan and was made by two brothers Basit and Amjad Farooq Alvi who were software vendors. The purpose of their virus was to find out the extent of piracy in their country, and it left a text message with their name, address and telephone number. This virus was spread by infected 360kb diskettes, and had infected IBM PC s worldwide by 1987.

The viruses Stone and Internet Worm (MORRIS) appeared in 1988. Stone was the first bootstrap-sector virus that infects the boot sector of a floppy disk. If the infected floppy was used as a boot disk, it then infected the master boot record. This meant that even if the whole hard-drive were formatted, it would still be infected. To get rid of the virus the master boot record had to be erased by using the utility called FDISK and loading the command FDISK /MBR . The Internet Worm Morris infected over six thousand computers in the USA alone, which infected institutes such as NASA. The virus was spread by making unlimited copies of itself and infecting computers over a large network.

In 1989 Russia was hit by an epidemic of viruses. First of all, there were two versions of the virus Cascade , followed by the Vacsina and Yankee viruses, then Vienna , Eddie , and then PingPong .

The first Polymorphic viruses appeared in 1990 Chameleon . The Chameleon Family of viruses are encoded, using two algorithms. The first algorithm contains the actual virus variants, and the second is the algorithm that complicates the viruses tracing.

The first Macro language viruses appeared sometime in 1995. (MS Encarta 98, Virus [computer], History) A macro language virus controls the functions of a legitimate program. It can infect any computer or operating system that can run the program .

The Development of Anti-virus Applications

About ten years ago, long after the introduction of the computer virus, certain companies started to make programs to combat the computer virus epidemic. These programs are called Antiviral Software . Antiviral software is used to scan system memory, the master boot record, and each and every file on a PC for the characteristics of a virus s code. Because the program knows what code it is looking for, infected files can usually be disinfected and return to, or as close to its original state. Antiviral software can only be effective if the virus definitions are updated regularly, as hundreds of new viruses are written every day. Antiviral software is not completely fool proof, as not all viruses are known of. As of 1995 when the first Macro viruses were introduced, programmers had to change the way their companies anti-virus programs scanned for viruses as a new technique had to be used to find these viruses, otherwise the viruses would go undetected.

The Current Status Of Microcomputer Viruses

The main types Boot , Program and Multi-partite (a combination of both boot and program) viruses are all still a threat to anyone who shares files from other computers, or who is connected to the Internet or a network. The major threat to computer users these days however, and since there introduction in 1995 is the family of Macro viruses. A macro is a set of keystrokes and instructions that can be saved in a single short key code (MS Encarta 98, Virus [computer], History). It is written in assembly language and can be used in legitimate programs such as Microsoft Word , Microsoft Excel , Microsoft Access , Microsoft PowerPoint , Lotus WordPro , Microsoft Outlook Express etc, just to name a few. These keystrokes and instructions are used to make a number of tedious and time-consuming operations in to one simple keystroke.

Evil and conniving programmers have found another use for the macro, and that is to turn it into a Virus by making a number of operations that can Reich havoc on your computer. This type of Virus can cause loss of your data, or even exploiting your privacy in programs such as Microsoft Outlook by stealing passwords or credit card numbers from your computer and giving them to the person that launched the virus. In Microsoft Outlook Express it usually makes a copy of all the people listed in your address book, and it then sends those people the virus as a document attachment in the e-mail. This pyramid of addresses from peoples address books is the reason why macro viruses made for legitimate e-mail programs such as Microsoft Outlook Express spread to so many computers and so quickly in just a short period of time. Major outbreaks in this type of virus have been the Melissa , I Love You and the Anna Kournikova viruses.

Details Of Recent Virus Outbreaks

The most recent and most major virus outbreaks of late, have all been from the Macro family of viruses. In 1999 the Melissa virus was in the wild and replicated under MS Office 97 and MS Office 2000 , using the e-mail program MS Outlook to spread. Kaspersky (www.avp.ch) The virus also has trigger routine, changes the system registry, disables Word macro-virus protection . This virus infects Word documents by changing the data format, and if the virus is run under MS Office 2000 , it has an extra action that disables MS Office 2000 anti-virus security, which can make it go undetected.

The I love You Bug , also known as I-Worm.LoveLetter is the next most recent major outbreak which was popping its ugly head up all over computers worldwide in the beginning of May 2000. Kaspersky (www.avp.ch) The worm spreads via E-mail by sending infected messages from affected computers . Once again, this is another virus that uses MS Outlook to steal contacts from your address book, and send everyone listed there the virus. This virus only works on systems that have Windows Scripting Host installed, but unfortunately Windows 98 and Windows 2000 have it installed by default.

The most recent outbreak was in February 2001, the Anna Kournikova virus, which is another virus sent as an attachment via the e-mail in MS Outlook . The file name for the attachment is AnnaKournikova.jpg.vbs , along with a message that entices the reader to open the file, claiming it to be an explicit picture of the famous Tennis Star Anna Kournikova . The virus infected computers worldwide, but it is said to have hit Australia the hardest with an estimated 100,000 computers infected by the e-mail (CNN.COM, 2001).

My Recommendations For Basic And Feasible Anti-Virus Measures

To be protected from the majority of harmful computer viruses, you need an Anti-virus Application of some description, with its virus definitions updated regularly for the best protection. I use a program called Antiviral Toolkit Pro , and I personally believe it to be the most affective. It s virus definitions are updated daily, and a full working version with a thirty day evaluation license can be downloaded from www.avp.ch . I also recommend that you should install more than one anti-viral application, as I have noticed that sometimes one program may detect a virus that the other may not, or even, one may do a better job disinfecting the infected files.

Other respectable anti-virus applications include Norton Anti-virus 2001 , in which an evaluation demo can be downloaded from www.symantec.com , and McAfee Anti-virus which can be downloaded from www.mcafee.com . All full versions of these can be bought from respectable retailers such as Harvey Norman etc.

Conclusion

In conclusion Macro viruses are the latest and greatest threat, so always be careful when opening up e-mail attachments. In this day and age, an anti-virus program of some description is a must have, as some protection is better than no protection at all. To have the most affective protection possible, a well-known and well-accredited anti-virus program is a need, not a want. This has to come with regularly updated virus definitions that can be downloaded from the Internet. If updated virus definitions cannot be updated regularly, then the anti-virus program should be rendered useless, as it cannot and will not protect you from the latest and meanest viruses. Although these programs cannot protect you one hundred percent from the thousands of new viruses that are written everyday, it will protect you from the main threats. Unfortunately viruses are here to stay!