Journal of American Science

Websites:
http://www.jofamericanscience.org
http://www.sciencepub.net

Emails:
editor@sciencepub.net
sciencepub@gmail.com

MARSLAND PRESS
Multidisciplinary Academic Journal Publisher

COMPUTER-VIRUS: TYPES AND ITS PREVENTATION

Dr. Vivek Kumar

Assistant Professor In Computer Science, Hari College of Management, Hindon Bridge, Dehradun Road, Gagalheri-247669, Saharanpur (Uttar Pradesh)
viveks865@gmail.com

Abstract: Chances are you've heard how important it is to keep viruses out, but what is a computer virus exactly? A computer virus is a type of malicious software, or malware, that spreads between computers and causes damage to data and software. Computer viruses aim to disrupt systems, cause major operational issues, and result in data loss and leakage. A key thing to know about computer viruses is that they are designed to spread across programs and systems. Computer viruses typically attach to an executable host file, which results in their viral codes executing when a file is opened. The code then spreads from the document or software it is attached to via networks, drives, file-sharing programs, or infected email attachments.

[Kumar, V. **COMPUTER-VIRUS: TYPES AND ITS PREVENTATION**. ***J AM SCI*** **2024;20(5):9-12]. ISSN 1545-1003 (PRINT); ISSN 2375-7264 (ONLINE). HTTP://WWW.JOFAMERICANSCIENCE.ORG02. DOI:10.7537/MARSJAS200524.02.**

Keywords: Computer, Virus, Types, Preventation

Introduction:

A computer virus is a kind of software that infects programs, data or dices and can reproduce itself in the same or other form. Despite all preventive measures, the viruses are becoming an order of the day. Viruses are enemies of computers and destroy whatever is stored in it, innocently, calmly and intelligently."

It was Fred Cahen who incidentally coined the expression 'Computer virus'. the term 'virus' and 'worm' used in science fiction novels in the early 1970's. Around the same period, researchers at Xerox Corp., created and demonstrated a self replicating code, called viruses.

A virus is a program that can modify another program is deemed infected. This can also become an evolved copy of the original virus program. Every program that gets infected may also act as a virus and thus the infection multiplies. The key property of a virus is its ability to infect other programs. Every general purpose system currently in use is open to viral attack in some secure systems, virus tends to spread further when created by some user of the system. A virus has the potential to spread throughout any system which allows sharing. The virus can be generated and introduced by a hacker. The perpetrator gets the satisfaction of demonstrating human superiority over a cybernetic system.

With the advent of Internet a haven has been created for virus mongers. An important ongoing research involves determining how quickly a virus could spread to a large percentage of computers in the world. Studies through simplified mathematical models of virus spreading in typical computer networks have been going on. Obviously virus-like programs have to be written, injected into systems and the effect has to be studied. in a simulated environment, the extent, speed and effect of infection is studied. Several experiments have been systematically carried out. The anti-virus program writers must be doing similar experiments before eventually bringing out their anti-virus packages.

Virus study indicates a set of 'undecidable detection problems'. A list could be as follows:

- Detection of a virus by its appearance.
- Detection of a virus b y its behaviour.
- Detection of evolution of a known virus.
- Detection of a triggering mechanism by its appearance.
- Detection of a triggering mechanism by its behaviour.
- Detection of evolution of a known triggering mechanism.
- Detection of a viral detector by its behaviour.
- Detection of evolution of a known viral detector.
- Safety of a protection scheme.

With networking becoming the order of the day, a virus may get initiated only though a particular node or through a few nodes and may give an appearance of having originated from some other node. A virus may also get kinglet at some stages of a

program in an executable file and not necessarily whenever the program is called for.

Experts say that a virus need not be used only for evil purposes. A very interesting theory in compression through virus has been developed. It can be explained that a simple virus can be written to find uninfected executable file, compress them and insert itself into them. Upon execution the infected program decompresses itself and executes normally. Studies indicate that such a virus could save over 50 percent of the space taken up by the executable files in an average system. The performance of infected programs decreases lightly as they are decompressed, and then the 'compression virus' implements a particular 'time space trade off'.

Another example could be that a virus program can be written in such a way to find 'uninfected' executable. It will plant itself fat their beginning. After a given date and time the virus could cause the executable to 'refuse service' by going into an indefinite loop. And in modern networking with the level of sharing that is prevalent, the entire system would become unusable as of that moment. Anti-virus operators might find a great a deal of hard work is required to treat/undo the damage caused by such a virus.

LITERATURE REVIEW

A virus is by definition a computer program that spreads or replicates by copying itself (F-Secure Corporation 2001). Computer virus attacks have become serious worldwide issue and can quickly spread through the Internet, causing even more damages (Joseph Wen 1998). Unlike other threats computer viruses able to infect from program to program, file to file and computer to computer very rapidly without direct human intervention. (Joseph Wen 1998) mentioned in his research that a computer virus can cause the loss or alteration of programs or data, and can compromise their confidentiality. (Joseph Wen 1998) stated that the vital part of a virus is a set of instructions that when executed spreads itself to other unaffected programs or files. Based on the intention of the virus developer these instructions can do any harmful activities like displaying a message, erasing files or altering stored data, replicating itself and taking up system resources such as disk space , memory, Central Processing Unit (CPU) time and network connections. (Joseph Wen 1998). In general most of the viruses are stay active in memory until we shut down our computer system. But when we turn off the computer we just temporarily remove the virus from memory, but not permanently remove from the file or disk it has infected. The next time when we use the computer system the virus program is activated and starts its vandal activities continuously. Typically there are many well-known techniques can be used by viruses to destruct the computer system. Basically a typical virus make two functions thus first it copies itself into uninfected programs or files, second it executes other malicious instructions the virus developer included in it. (Babak Bashari Rad et al, 2011) mentioned in their research that, there is a great fight between virus developer and anti-virus experts and it is becoming more difficult issue in day by day and in future too. (Essam Al Daoud et al, 2008) mentioned that anti-virus softwares are advancing their methods and techniques to detect viruses, on the other hand the virus developers are looking for new tactics to break them. Specially computer virus developers apply many strategies to escape from the detection such as space filling, compressing and encryption. On the other hand the antivirus softwares are trying to detect the viruses by using alternative static and dynamic methods. In general PC users today need to have a fully-fledged virus protection mechanisms to face the growing threat of virus attacks

TYPE OF VIRUSES

Non-TSR file virus:

This is the simplest form of virus to write-and the least effective, so one is unlikely to be troubled by them. When an infected program is first run, the virus code carries out its task checking that an executable file in not infected, then attaching a copy to it. It then runs the original program to which it is attached. In contrast, TSR viruses load themselves into memory when they are executed and are able to infect any executable program they can reach from that point.

Boot sector Virus:

This is the other major type of virus. Most of the boot sector consists of a simple, small program that is used to start DOS, or whatever operating system is installed. Boot sector viruses replace this with virus code and typically move the boot sector to another part of the disc. When the PC boot, the virus code is executed first. Then he virus runs the real boot sector. A very slow boot from an infected floppy with an excess of floppy dise activity is a common of an infect ed machine.

Multipartite Viruses:

These combine both techniques. They can infect both boot sectors and files. The file version of 'Tequila' , for example the Master Boot Record. Once the PC has been booted from an infected MBR, the virus goes memory resident and infects all accessed, EXE files.

Companion Viruses:

Companion viruses create a .COM companion to an. EXN file. Because DOS executes. COM files before. EXEs. The virus is run before the, EXE file of the same name. The virus then runs the original, EXE.

Polymorphic Viruses:

These aim to foil anti-virus packages that search for a specific strain by looking for a known sequence of bytes, no two copies of a true polymorphic virus are alike. When polymorphic viruses run they first decrypt themselves and then behave like any other virus. Programs such as the 'Nuke Encryption Device' (NED) and the 'Trident Polymorphic Engine' have been written that turn a standard virus into a polymorphic virus. Fortunately, once measures have been taken by an anti-virus company to defeat each 'engine', all viruses processed by it are detectable.

Stealth:

Stealth covers a variety of techniques that viruses use to disguise their presence from anything as simple as hiding the increase in files size of executable to full-blown detection of the tools used to detect the virus and the taking of appropriate action to fool them.

Trojans:

Trojans are not viruses at all. They are programs that hide a malevolent code within a seemingly innocuous program but they do not replicate. For this reason the chances of being caught out accidentally by Trojans area low.

Macro Viruses:

Macro viruses have been predicted for a while. It was recently appeared when it was sent out accidentally by Microsoft on a CD-ROM to OEMs. They called it a 'Prank Macro'. It is the first virus that will run on both PCs and Macs. It replicates using an auto-executing Word Basic macro embedded in a document. When the document is loaded, it copies the macro to Word's settings file NORMAL, DOT, and replaces the file save command with a routine that also saves a copy of the macro in each document.

PREVENTION FROM A VIRUS ATTACK

The most fundamental precaution against virus attacks is to limit access to a machine to avoid tamper with the system. In case of floppy discs, the simplest form of protection is to place write-protect tabs on all discs so that any attempt by a virus to write to the dice would result in an error message. The write-protect tab should be removed only when data has to be expressly written to the floppy.

It should be remembered that even the simple act of inserting a floppy disc and getting a directory listing could be enough to infect a machine. Though write-protect facilities are generally not available for hard discs, hardware products have started appearing in the market offering users the ability to write-protect hard discs. But being expensive, these are not likely to be used widely.

Software products to write-protect hard discs are also available. But these render themselves vulnerable to virus attack also. In network environments, the use of diskless or hard-disc-only systems is becoming popular. Control of software is then restricted to the file server and network administrators only.

Tips for Prevention of Virus Infection

Even if one buys and uses several anti-virus applications, the best defence is to avoid infection in the first place. There is no absolute guarantee against infection. But the risk can be minimised by following the guidelines listed below:

- Boot the system with a write-protected and already scanned floppy disc, which has the boot and system files and set of files of a qualified virus scanned program.
- Even if there is a hard disc and the PC normally boots from that disc, start by first booting the system with the uninfected and write-protected disc boot floppy in the 'A' drive.
- All floppies should be scanned individually and periodically by using a qualified and uninfected virus-scanning (or detection) program.
- Discourage the use of floppies of other users unless these are individually scanned and specked for any virus.
- Do not use previously formatted floppies brought by others even if these are apparently empty. Reformat all empty floppies with your uninfected system before further use.
- Avoid lending floppies.
- The most popular carriers of dangerous viruses are floppies containing different popular computer games, horoscopes, astrological predictions etc. These should be avoided.
- Use of pirated software should be completely avoided, as most of them are virus carriers.
- Take back-ups regularly. A full back up once a week, with incremental back-ups daily, if necessary, is advisable. Uninfected back-ups allow overwriting infected files. Even infected back-ups permit recovery from logic bombs. Disinfect restored files right away.

- Write-protect and back up the installation discs before installing any new software. If it is not done and the system already has virus infection, the original program discs could be permanently infected during installation.
- Scan network drives used regularly. The files attached to E-mail messages may be infected.
- Use the memory-resident, virus-spotting portion of the anti-virus application at all times. If an infection is suspected, turn off the system immediately. Reboot from a clean floppy (one without an FAUTOEXEC.BAAT OR A CONFIG. SYS file). Then disinfect the system using a disc-based copy of the anti-virus program.

User should also have some basic knowledge about viruses, their prevention and cure. Use of good anti-virus software for scanning files regularly should invariably be used by each and every user.

But single software cannot be depended upon to eliminate infection from all strains of viruses. The battle against virus infection will be long and perhaps, lasting.

References

[1]. A. Coulthard and T.A. Vuori (2002), Computer Viruses: a quantitative analysis Logistics Information Management, Volume 15. Number 5/6. 2002. PP.400- 409, ISSN 0957 - 6053

[2]. Ajayshivaa (2007). Symptoms of virus attacks [Online] February 28, 2007. Available from : http://www.astahost.com/info/tiposc-symptoms-virusattack.html. [Accessed: 20th May 2013]

[3]. Babak Bashari Rad, Maslin Masrom and Suhaimi Ibrahim (2011), Evolution of Computer Virus Concealment and Anti-Virus Techniques: A Short Survey, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 1

[4]. Essam Al Daoud1, Iqbal H. Jebril and Belal Zaqaibeh (2008), Computer Virus Strategies and Detection Methods, Int. J. Open Problems Compt. Math., Vol. 1, No. 2,

[5]. Frederick B. Cohen and Sanjay Mishra (1992) "Experiments on the Impact of Computer Viruses on Modern Computer Networks"

[6]. F-Secure Corporation (2001), "Computer Viruses – from an Annoyance to a Serious Threat". White Paper Joan C. Hubbard, and Karen A. Forcht (1998), Computer viruses: how companies can protect their systems, Industrial Management & Data Systems, MCB University Press ISSN 0263-5577

[7]. Joseph Wen H (1998), Internet computer virus protection policy, Journal of Information Management & Computer Security 6/2 66–71 MCB University Press. ISSN 0968-5227

[8]. Kendria (2011). Types of viruses and their effects on your PC [Online] April 7, 2011.Available from: http://techgyo.com/index.php/types-viruses-effects-pc. ccessed: 22th May 2013]

4/25/2024