INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

Computer Virus: A Major Network Security Threat

Sivanandam Natarajan
Department of Computer Engineering
Suguna College of Engineering, Coimbatore, Tamil Nadu, India
S. Rajarajesware
Department of Computer Engineering
Sree Narayana Guru Polytechnic College, Coimbatore, Tamil Nadu, India

Abstract:
Computer viruses and worms have been becoming important security threats, over several decades. At present in any organization using computers it is a challenging task to identify and rectify the problems caused by the viruses. This paper begins with the basic structure and mechanisms of computer viruses. Here we present an overview on computer viruses and the different types of threats due to various viruses to the existing computer networks. The sample signature of few viruses is also given.

Keywords*: Virus, Worm Malware, Signature, Detection, Mechanism*

1. Introduction

A computer virus is a computer program that can copy itself and infect another computer without the permission or knowledge of its user [1]. The computer viruses have the capability of spreading from machine to machine and are typically done without the user's knowledge or permission. Viruses add their code to other systems in such a way that whenever the infected part of the system executes, the viral code is also executed and the virus spreads further. An important primary characteristic of computer viruses is their ability of either to reproduce themselves or to produce an altered version of themselves [2].

Normally all virus programs are written in such a way that they perform examinations of their host environments as part of their activities. They seek weak points to alter interrupts, examine memory and disk architectures, and alter addresses to hide themselves and spread to other hosts. They can also alter their environment to support to hide their existence. Computer viruses run on a variety of machines under different operating systems.

During the early stages of virus creation, virus programmers tried to infect a large number of victim systems throughout the world with similar type of infection mechanism, but the malicious actions performed were different. Viruses were created to corrupt the disk system, system programs and application programs, email accounts, various networks, etc. The methods used to infect a host machine and spread to other machines were similar for all these viruses. Virus detection systems attempted to detect the infections based on the signature files and actions performed by viruses. Most of the early stage viruses were detected based on their signatures. At present, the virus programmers started implementing new methods for creating and spreading viruses and thus cause serious infections.

During recent years, the number of malicious programs attacking computer networks has been growing rapidly. According to security experts, the number of viruses will be more than a million in the near future. Though the number of viruses has drastically increased, patches and removal tools for most of the viruses have been created and they were not sufficient to completely recover from the threats due to viruses. The computer virus writers use many strategies to evade detection like space filling, compression, encryption and other code transformation techniques. All the available antivirus software's were trying to detect and remove the viruses by using various methods. However; all the existing methods are not adequate as new viruses are coming rapidly.

Studies and researches show that computers connected to the Internet may experience an attack in less than every 39 seconds and new vulnerabilities in the system are arising continuously.

These vulnerabilities like installing malicious programs on user machines create lot of problems such as loosing data or modifying data, Denial of Service attacks, etc. Unfortunately, our current ability to defend against new viruses is extremely poor as the complexity of modern viruses and worms are making this problem more difficult.

Thus, an intelligent threat identification and intrusion detection systems are necessary to handle different types of viruses.

2. Types of Computer Viruses

The classification of computer viruses can be done via several ways based on the type of host victim, type of infection technique, etc. Few of the computer viruses are briefly given here [6]:

Virus Name	Brief note on the virus
Boot Sector Virus	This virus takes advantage of the executable nature of master boot record (MBR) and partition boot sector (PBS). A PC infected with a boot sector virus will execute the virus code when the machine boots up. **Michelangelo virus** is an example of a Boot Sectors Virus. The only way that a system can become infected with a boot sector virus is to boot the system using an infected floppy disk.
File infecting viruses	File infecting viruses infect files and sometimes they may be memory resident. They will commonly infect either most or all of the executable files (those with the extensions .COM, .EXE, OVL and other overlay files) on a system. Some file infecting viruses will only attack operating system files (such as COMMAND.COM), while others will attack any file that is executable. Example: Sunday and cascade viruses.
Multi-partite viruses	Multi-partite viruses are those that infect both boot sectors and executable files. They are the worst viruses of all because they can combine some or all of the stealth techniques, along with polymorphism to prevent detection..Example: Invader and Flip viruses
Shell viruses	A shell virus is one that forms a "shell" (as in "eggshell") around the original code. During execution, the virus becomes the original host program, and the original host program becomes an internal subroutine of the viral code. Shell virus moves the original code to a new location and takes on its identity. When the virus is finished executing, it retrieves the host program code and begins its execution..Almost all boot program viruses are shell viruses.
TSR viruses	TSR stands for **Terminate and Stay Resident [4]**. This term was often used with the Disk Operating System. These are also considered memory resident. In the computer world a program can install them in memory, and this part can remain active after the program has ended. This memory resident part is called as resident extension. Many viruses install themselves as resident extensions.
Overwriting Virus	This type of virus overwrites files with their own copy. Of course, this is a very primitive technique, but it is certainly the easiest approach of all. Overwriting viruses cannot be disinfected from a system. Infected files must be deleted from the disk.
Appending Virus	This type of virus uses a technique in which the code contains a jump (JMP) instruction, inserted at the front of the host to point to the end of the original host. A typical example of this virus is Vienna.
Prepending Virus	This virus inserts its code at the front of host programs. This is a simple kind of infection, and it is often very successful. Virus writers have implemented it on various operating systems, causing major virus outbreaks in many. An example of a COM prepender virus is the Hungarian virus Polimer.512.A, which prepends itself, 512 bytes long, at the front of the executable and shifts the original program content to follow itself.
Macro virus	This infects a Microsoft Word or similar application and causes a sequence of actions to be performed automatically when the application is started or something else triggers it. Macro viruses tend to be surprising but relatively harmless. A typical effect is the undesired insertion of some comic text at certain points when writing a line. A macro virus is often spread as an e-mail virus. Example: Melissa virus.
Email viruses	This type of viruses are activated and spread in systems when an email attachment is opened. Example: ILOVEYOU virus.
Polymorphic Viruses	Polymorphic viruses try to bypass virus detection systems by mutating themselves through self-encryption. The code encryption implemented in polymorphic viruses hides the signature of virus files. The code is encrypted using different keys to hide its existence at the victim host machines. The decryption engine is attached in the code itself, which will then decrypt the code and execute the virus. This type of viruses is harder to detect since signature is hidden using encryption. Example: stimulate, Phoenix viruses

Table 1: Types of Computer Viruses

3. Structure and mechanism of Virus

A computer virus has the following basic and necessary components [8]:

- Search routine
- Copy routine and
- anti-detection routine

All the above routines are shown in the following Figure:

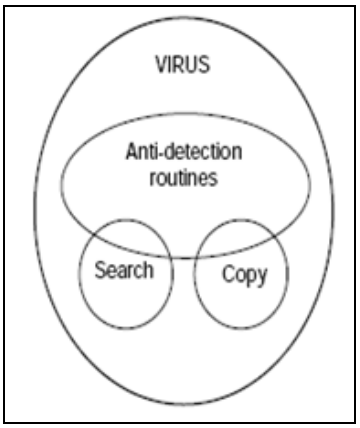

Figure 1: Functional diagram of a simple virus (initially developed viruses)

Initially Assembly language is used to create virus when DOS was the only operating system widely used in the world. Besides this assembly language virus programmers are using other languages including VB and Java scripts. The Virus programmers technically used the ISRs (Interrupt service Routines) in DOS to run viruses. Interrupt 21H is the main DOS interrupt service routine that we will consider. To call an ISR, one simply sets up the required CPU registers, and calls the interrupt. For example, the following code opens a file whose name is stored in the memory location FNAME in preparation for reading it into memory

```
mov ds,SEG FNAME ;ds:dx points to filename
mov dx,OFFSET FNAME
xor al,al ;al=0
mov ah,3DH ;DOS function 3D
int 21H ;go do it
```

The “int 21 H” instructions transfers control to DOS and allow it do its job. When DOS is finished opening the file, control returns to the statement immediately after the “int 21H”. The register **ah** contains the function number. The other registers must be set up differently, depending on what **ah** is, to convey more information to DOS about what it is supposed to do. In the above example, the **ds:dx** register pair is used to point to the memory location where the name of the file to open is stored. register **al** tells DOS to open the file for reading only.

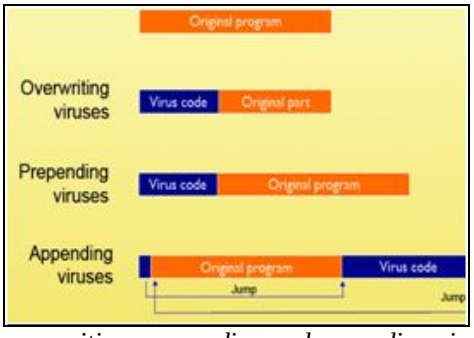

Figure 2: Effects due to overwriting, prepending and appending viruses on orignal program

4. Signature

A signature is a sequence of bytes extracted from the body of the virus or worm. Most of the virus programmers add *signature* to their program. So by checking the signature, we can find the name of the virus. Most of the anti-virus packages use this logic. But it is a fact that checking out the *signature* is not always 100% foolproof.

The following table shows some of the viruses and their *signatures [3]*.

Name of the virus	Signature
Boot-Dropper	ad920a165c008d32b80103565152cd13
Cascade-YAP #1	0f8db74d01bc800631343124464c75f8
Christmas	bcca0afce80300e97d05505156be5900b91c0990d1e98ae1
Einstein	0042CD217231B96E0333D2B440CD2172193BC17515B80042
Necropolis	50FCAD33C2AB8BD0E2F8
Vienna #1	8bf283c60a90bf0001b9 [AND] 8bf283c60a90bf0001b903
Vienna #2	fc8bf281c60a00bf0001b90300f3a48b
W32/Beast	83EB 0274 EB0E 740A 81EB 0301 0000

Table 2: Signature of few viruses

5. Conclusion

Today almost all of the existing computer networks are facing lot of threats. Malwares are important causes for threats in computer networks. Computer Viruses are coming under the category of malwares and they cause lot of threats to the system security, integrity and efficiency. The computer viruses can be detected by different methods. As computer viruses use different mechanisms, a single detection method is not suitable to detect all the available viruses..All the existing methods cannot provide guarantee to detect all viruses as new viruses and worms with different strategies are coming rapidly. So some improvement should occur in future and that also cannot provide guarantee to detect all viruses because by that time some more new viruses may arise. This remembers Newton's third law, "for every action there is an equal and opposite reaction". Our new methods simulate the actions and advent of new viruses and vulnerabilities simulate the reactions with respect to Newton's third law of motion.

6. References

1. http://guideme.itgo.com/atozofc/
2. http://en.wikipedia.org/wiki/Computer_virus
3. http://www.nlnetlabs.nl/downloads/antivirus/antivirus /virussignatures.strings
4. http://library.thinkquest.org/C005965F/viralinfo/tsr.htm
5. Babak Bashari Rad, Maslin Masrom and Suhaimi Ibrahim, "Evolution of Computer Virus Concealment and Anti-Virus Techniques: A Short Survey" ,IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 1, January 2011
6. Bhaskar V. Patil, Dr. Milind. J. Joshi, "The Working and Problems of Computer Virus in Enterprise Areas" International Journal of Computer Science and Information Technologies, Vol. 2 (4) , 2011, 1789-1792
7. Asmaa Shaker Ashoor, Prof. Sharad Gore, Prof. Vilas Kharat, "Computer Viruses in UNIX Environment: Case Study"IJCES International Journal of Computer Engineering Science , Volume1 Issue 3, December 2011
8. Mark A. Ludwig "The Little Black Book of Computer Viruses", Volume One,The Basic Technology,American Eagle Publications, Inc.,1996.
9. Essam Al Daoud1, Iqbal H. Jebril2 and Belal Zaqaibeh –"Computer Virus Strategies and Detection Methods",Int. J. Open Problems Compt. Math., Vol. 1, No. 2, September 2008
10. P. Szor, P. Ferrie, "Hunting for Metamorphic," Symantec SecurityResponse. http://www.symantec.com/avcenter/reference/hunting.for.metamorphic.pdf.
11. A. Walenstein, R. Mathur, M.R. Chouchane and A. Lakhotia, "Normalizing Metamorphic Malware Using Term Rewriting," Proc. Int'l Workshop on Source Code Analysis and Manipulation (SCAM), IEEE CS Press, Sept. 2006. Pages 75–84.
12. "Benny/29A",Theme:metamorphism, http://www.vx.netlux.org/lib/static/vdat/epmetam2.htm
13. P. Szor, "The Art of Computer Virus Defense and Research," Symantec Press 2005.
14. A. Venkatesan, "Code Obfuscation and Metamoprhic Virus Detection,"Master's thesis, San Jose State University, 2008