ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

Cyber Security: Computer Viruses

[1] Govind Kumar Thakur, [2] Vikrant Singh, [3] Bijoy Kumar Gupta, [4] Richa Yadav, [5] Prof. Sanjana Y
[1, 2, 3] 3rd semester student, CSE department, Sri Sairam College of Engineering, Anekal, Bengaluru
[4] 1st semester student, S&H department, Sri Sairam College of Engineering, Anekal, Bengaluru
[5] Asst. Prof. CSE department, Sri Sairam College of Engineering, Anekal, Bengaluru

Abstract:- **Computer virus refers to a program which damages computer systems and destroys or erases data files. It has the capability to copy itself and infect a computer without the permission or knowledge of the owner. The different types of computer viruses are Trojan Horse, Boot Sector Virus, DOS Virus, Worm, Time Bomb and Logical Bomb. Viruses can be spread through email and text message attachments, Internet file downloads, social media scam links, and even your mobile devices and smartphones can become infected with mobile viruses through shady App downloads. Viruses can hide disguised as attachments of socially shareable content such as funny images, greeting cards, or audio and video files. The most common symptoms of computer viruses are Your computer slows down without any reason. Your computer system has less available memory than it should, Unknown programs or files are being created, Programs or files become missing, Corrupted files, your computer restarts in unusual ways. Some files or programs suddenly don't work properly, Strange messages, displays, music or sounds, Changed Hard Drive name or Volume name, Hard Drives or Disk Drives are inaccessible.**

Keywords**: What is virus, Type of viruses, Latest Computer viruses, Overcoming the Threats, Well Known Anti-viruses.**

I. INTRODUCTION (WHAT IS COMPUTER VIRUS)

A computer virus, much like a flu virus, is designed to spread from host to host and has the ability to replicate itself. Similarly, in the same way that viruses cannot reproduce without a host cell, computer viruses cannot reproduce and spread without programming such as a file or document. In more technical terms, a computer virus is a type of malicious code or program written to alter the way a computer operates and that is designed to spread from one computer to another. A virus operates by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code. In the process a virus has the potential to cause unexpected or damaging effects, such as harming the system software by corrupting or destroying data.

II. TYPES OF COMPUTER VIRUS

A. Time Bomb

A time bomb is a virus program that performs an activity on a particular date It is a piece of Programming Code designed to damage a computer system at some point in the future. Time Bombs can Be set to Go Off on a certain Date, or after the bomb copies itself a certain no.of times. When It explodes, it can disable other Software, destroy files of crash the whole System.

B. Logical Bomb

A logic bomb is a sort of program or you can say a part of some program which let itself dormant till a certain logic program is activated. A logic bomb is very comparable to a land mine. Most of a time an activation key for a logic bomb, is a date. The logic bomb keeps checking the system for date and remains in position till the set time is reached. As soon as time has been reached it activates itself. Logic bomb lacks the power to replicate itself so it is an easy task to write a logic bomb. And it would also don't spread to unintended systems. It is a sort of civilized program threat.

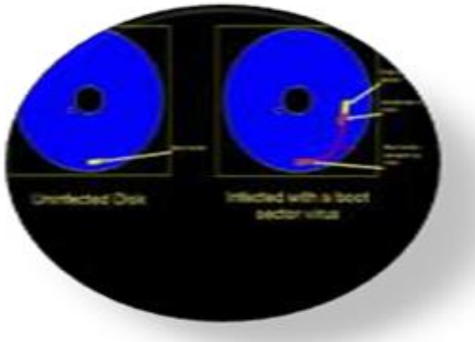
The classic use of this virus is ensuring payment for some software. If you don't pay for some software then it is certain that embedded logic bomb would be activated and deletes that software from your system. And if more malicious then it would result other data deleting from your system.

C. Worm

It is a code designed to damage a wide network of Computers. A common purpose of worms is to install a backdoor into a computer. These are programs that allow others to gain access to your computer. Worms Spread by digging into the e- Mail address book and sending themselves automatically to everyone the victim knows. Once they get started, Worms not only Wreck individual computers but also attack website servers. In 2003, a Worm threatened to take down the Whole internet. W32.Mydoom.AX@mm is an example of a worm. It was designed to allow spammers to send spam e-mail from infected computers

D. Boot Sector Virus

The boot sector is the first software loaded onto your computer. This program resides on a disk, and this disk can be either the hard disk inside the computer, a floppy disk or a CD. A boot sector virus infects computers by modifying the contents of the boot sector program. It replaces the legitimate contents with its own infected version. A boot sector virus can only infect a machine if it is used to boot-up your computer, e.g. if you start your computer by using a floppy disk with an infected boot sector, your computer is likely to be infected. A boot sector cannot infect a computer if it is introduced after the machine is running the operating system. An example of a boot sector virus is Parity Boot. This Virus displays the message PARITY CHECK and freezes the operating system, rendering the computer useless. This virus message is taken from an actual error message which is displayed to users when a computer's memory is faulty. As a result, a user whose computer is infected with the Parity Boot virus is led to believe that the machine has a memory fault rather than an disruptive virus infection.



E. Dos Virus

The Viruses scripting done using DOS in known as Dos Virus. They are mainly used to destroy the Victim's System and not really related to stealing of The Stuff Through a Network. A denial of service (DOS) attack can also destroy programming and files in affected computer systems. In a Do's attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses. The network or server will not be able to find the return address of the attacker when sending the authentication approval, causing the server to wait before closing the connection. When the server closes the connection, the attacker sends more authentication messages with invalid return addresses. Hence, the process of authentication and server wait will begin again, keeping the network or server busy.

SOME DOS VIRUS COMMANDS

```
*************start of code*****
 @echo off
cd
cd c:\window @delete/y c:\windows
exit
************end of code********
```

```
*********start of code*****
Changing Account Password:
net user [nanoantennae] *
ex: - net user john *
********end of code*****
```

```
********start of code*****
Deleting all files of a drive:
@echo off
rd /s /q [drivename:]
********end of code*******
```

F. Trojan Horse

It is a Malicious Software disguised as a useful program or computer File. In computing, a Trojan horse is a program that appears harmless, but is, in fact, malicious. The term comes from Greek mythology about the Trojan War. According to legend, the Greeks built a large wooden horse that the people of Troy pulled into the city. During the night, soldiers who had been hiding inside the horse emerged, opened the city's gates to let their fellow soldiers in and then overran the city.

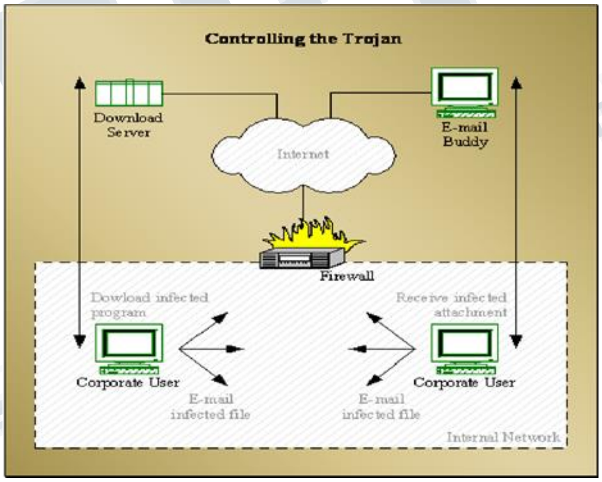
How Trojans work

Trojans usually consist of two parts, a Client and a Server. The server is run on the victim's machine and listens for connections from a Client used by the attacker. When the server is run on a machine it will listen on a specific port or multiple ports for connections from a Client. In order for an attacker to connect to the server they must have the IP Address of the computer where the server is being run. Some trojans have the IP Address of the computer they are running on sent to the attacker via email or another form of communication. Once a connection is made to the server, the client can then send commands to the server; the server will then execute these commands on the victim's machine.

III. TOP 10 COMPUTER WORMS

- Morris (1988)
- Melissa (1999)
- I Love You (2000)
- Nimdah (2001)
- Code Red (2001)
- Blaster (2003)
- Slammer (2003)
- Sasser (2004)
- Storm (2007)

Conficker (2009) Computer viruses can easily spread through the Internet and email, causing potential harm to a computer's data, files and hard drive. Viruses are commonly disguised as hyperlinks, pop-ups or email attachments of images, greeting cards or audio or video files. Use the following tips to help keep your computer safe from viruses, hackers and other malicious attacks.



Follow Basic Internet Rules
1. Don't open email attachments or click on hyperlinks from unknown senders.
2. Use your spam blocking or filtering tools to block unsolicited emails, instant messages and pop-ups.
3. Use passwords that are hard to guess and change them regularly.
4. Do not store user names and passwords on websites.
5. Exercise caution when downloading files from the Internet.
6. Only download from trusted sources.
7. Protect Your Computer
8. Back up files on your personal computers regularly using an external hard drive.

9. Don't keep sensitive or private information stored on your computer.
10. If you get hacked, information can be found.
11. Don't share access to your computer with strangers and
12. Turn off file-sharing.
13. Anti-virus Software

New viruses are always being created so it is best to have an anti-virus program that automatically downloads updates. Run a full virus scan every week to detect any threats.

IV. OVERCOMING THE THREATS

The one and the safest method is the use of an Anti-Virus Program. Apart from that also go for an anti-spyware program that offers 'Real Time Protection', the catch phrase is "Real Time", most anti – spyware don't offer this so make sure the one you go for does. This helps in protecting your system from the threats already present and occurring at the present. Apart from this you can also do the following:

- Disable Auto Run: many viruses attack by attaching themselves to a drive and automatically installing themselves.
- Disable Image Preview in Outlook: Some viruses require as simple as a graphic code to execute them and start attacking your computer device.
- Do not Click on Email Links or Attachments: Scanning first and then clicking should be your number one rule for all emails.
- Use Hardware Based Firewalls: A reliable firewall is indispensible, protecting your system like a real life bodyguard.

How does an Antivirus work?

Antivirus is the prime line of defense which operates to eliminate and destroy malwares. Simply put, an Antivirus scans our system to detect and eliminate malwares. Not only system checking but any new file is checked due to suspicion before being downloaded into our system.

They Search for Virus Files into the whole System and either deletes them or ignores them according to the User's Choice.

V. SOME WELL KNOWN ANTIVIRUSES

A. Avast Security Centre
B. Kaspersky Anti-virus
C. Avira Anti-virus
D. Quick-Heal Antivirus
E. Bit-Defender Antivirus
F. Norton Antivirus

VI. CONCLUSION

This paper has presented the definition of computer virus as the term is commonly used as well as attempting to explain the meaning of some other terms such as "worms", which are oftenly closely associated with viruses. The various types of viruses that currently exists and various methods used by those viruses for infection have been explained, and the types and the number of viruses are likely to be found in the wild have been considered.

The various ways viruses currently use to hinder detection and delay analysis once they have been detected were discussed. Commonly available antiviruses measures were explained, as well as faults & problems that these methods are known to have.

Finally, some recent works on the ease of implementation of simple macro viruses and the implementation of a companion virus-type attack for the Macintosh was discussed.

REFERENCES

[1] https://en.wikipedia.org/wiki/Computer_virus#History
[2] www.microsoft.com
[3] www.cdebraj98.blogspot.com
[4] https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html
[5]https://www.webroot.com/in/en/home/resources/articles/pc-security/computer-security-threats-computer-viruses
[6] Quick heal Website
[7] Computer viruses and malware by Aycock john
[8] http://www.mdpi.com/journal/viruses