Zulkifl et al LGURJCSIT 2019

ISSN: 2521-0122 (Online)
ISSN: 2519-7991 (Print)

LGU Research Jounral for
Computer Sciences & IT

Vol. 3 Issue 3, July - September 2019

Computer Viruses, Attacks, and Security Methods

Muhammad Zulkifl Hasan [1] Senior Lecturer, M Zunnurain Hussain [3], Senior Lecturer Bahria University Lahore Campus[3], Zaka Ullah [2] Senior Lecturer Lahore Garrison University [1,2].

Abstract:

with the fast growth of the Internet, computer threats and viruses have become a very serious issue for us, which attract public attention. Therefore, the distribution of computer viruses and worms were discussed in this study. This paper focuses on the effects of computer viruses. The main area of this paper is a brief discussion on computer viruses and security or detection methods. This study is very useful and helpful for computer users to use the different methods, possible steps to protect their system and information from any kind of possible attacks on their system.

Keywords: computer threats, computer viruses, the risk of attacks, risk category, risk factors, cyber-attacks computer security methods

1. INTRODUCTION

During the past, a huge range of computer viruses and computer applications have become problematic issue for the computer system and network security. A computer virus is a computer program that executes when a contaminated program is executed. A computer virus reproduces its own code by linking itself to other files in a way that execute code when the infected executable program is executed.
It connected itself in the form of the host such as authorized, executable files. The virus exists inside the program, which said to be 'infected'.
Execution of host files indicates execution of the virus. It may or may not destroy or damage the infected program. The virus is capable to repeat itself and create copies of itself. It wants to have some method of spreading such as via computer network or disks.

Example: Sampo & Hare, W95.CIH (Chernobyl).

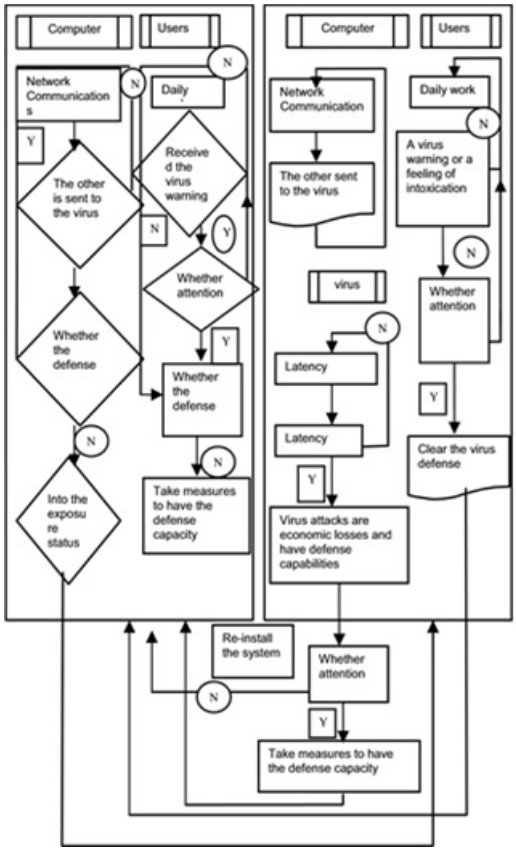

Figure 1 Flow chart

[Communication process by a computer, user behavior, & virus may form]
The distribution of computer virus is mostly through the disk boot sector, files, network communication and so on. Worms distribute mostly through the network. The illegal nature of computer viruses has many sorts like destructive, latent, hidden, triggered, variability, and unpredictability .

New tricks and new ways of virus spreading has appeared with the popularity of the internet. By using these ways viruses spread more rapidly this development can be very upsetting Therefore, the question is that how we solve security problems affected by the virus and how we improve the efficiency of system security and protection device for actual management of security this has become a huge challenge for a computer system.
Computer virus broadcast model was established and the distribution of computer viruses in different time structures and growth style replicated.
History- There are many stories of the first computer virus. The first large spread virus was IBM Compatible virus. Apple virus one 1981 is a boot sector infected virus which was developed for pirated games.
Classifying Computer Viruses- we discuss the general classified computer viruses that are Boot Sector, Multipartite, Terminate and stay resident (TSR), Polymorphic, Macro, Companion.
Moreover, after that, we discuss the major types of computer viruses' worms, Trojan horse, bombs, threats, discussed some attacks like denial of service attack or distributed denial of service attack including methods on infections and a brief discussion on computer security or prevention methods.
In Fig 2 shows the diagram of a computer virus, which has copy, search, and anti-detection system to avoid any type of detection from anti-virus program in Fig. (2,3) that are presents numbers of update which anti-virus program provide to its end users, which is growing every month.

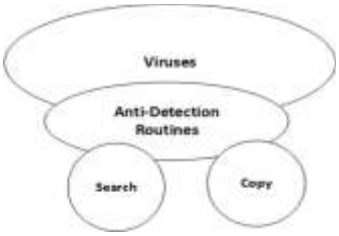

Figure 2 :A functional graph of a computer virus, which has a copy, search and anti-detection routine to avoid any identification from antivirus software.

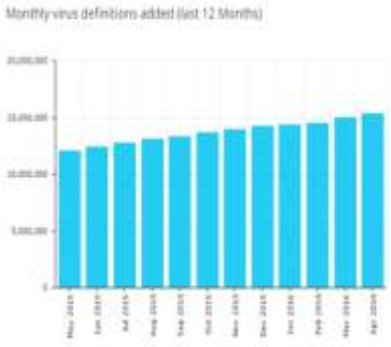

Figure 3 : The increase in user update for a computer virus in the last 12 months.

The paper encompasses the following:
1. Examine the different types of computer virus's distribution platform based on their use.
2. Presenting the virus spread opposition and demonstrate the major type of viruses.
3. Evaluating the viruses and prevention tools to secure the users by our security methods.

2. Methodology

Boot Sector- are those type of viruses that destroy or harm the boot sector or master boot record on a computer. At first, they move and overwrite the original boot program by changing it with infested boot code. After that, they move the original coding of the boot to another sector on the disk. This virus is very difficult to detect. It is the first thing loading when we start the computer.

Sometimes viruses are resident in memory. However, they generally infect executable file like.EXE, OVL, COM and other files on the system.
Terminate and stay resident (TSR) - Virus that stay active in storage after application or disk mounting, or bootstrapping. TSR is the virus that can be executable infector or boot sector infector.

Polymorphic- It changes their appearance with infection. This encrypted form of viruses is very difficult to detect because they are very good at

hiding themselves from antivirus programs. We can say that this virus is a hidden or encrypted form of viruses.

How virus work? Once computer virus gain access to the effects of these attacks, they possibly include:

- Flashing BIOS
- Destroy data or format hard drive
- Denial of service attack
- Distributed denial of service attack
- Replicating itself
- Network use or Interrupting system
- Using network resources or using a computer
- Spread confidential information
- Modifying or changing the configuration setting

Fig. 4. show how virus works and harm the computer system by running or executing illegal or harmful instruction. At first virus enter in the cell body releasing or exerting RNA and the virus RNA invades cell nucleus and take over. The viral RNA uses the host cell to make new RNA or assemble more viral particles. After that, new viral particles are released or sometime destroying the cell in the process, through this process virus is distributed in computer system.

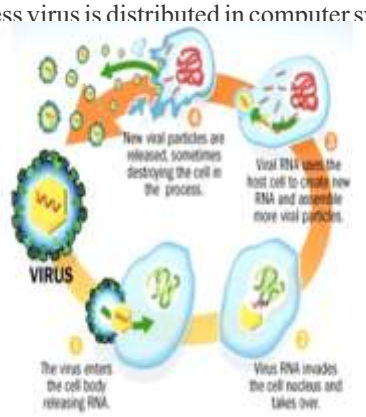

Figure.4 : How does virus work?

(a) Methods of Infection:

- Through removable media or removable devices
- Through downloading files
- Through the e-mail attachment
- Through-unpatched services or unpatched software.
- Through the poor administrator password
- Through the poor shared password

By these methods, infection occurs in user system or devices that can easily harm the entire system or prove it be a big cause of damage data.

Virus Distribution Platform- Depend on internet virus distribution. Instead of physically linked wireless or wired medium a logically linked network is use. The scale of virus broadcasting is restricted in this platform. According to the different application the major type of distribution platform, consist of free scale platform. All these methods are involved in the vulnerabilities process of the system.When the user is on internet or surfing site he/she don't know how much threat the system faces during surfing.

Phishing- It is the fraudulent act to obtain sensitive information or data like password, usernames and credit card detail by using secret or hiding tools as a trustworthy unit. E.g., Email fraud.

Malware- This attack is a piece of infected program that extracts over a personal computer in instruction to spread bug against other people devices and profile. Some types of malware include- adware, rootkits, Trojan horses, bugs, viruses, worms, and bots.

Eavesdropping Attack-, which is also known as snooping and sniffing. For example, open public Wi-Fi is an easy target for eavesdropping attack.

Redlof- is a polymorphic virus in the script of visual basic. It based on Microsoft ActiveX Component to run itself. It locates Folder.htt and harm that folder or file. Folder.htt is a chunk of Microsoft Active Desktop feature.

Trojan Horse- hides as very useful software or program in a computer. Trojan horse consists of hidden instructions to remove or erase data and cause other harm. For example, Format c.

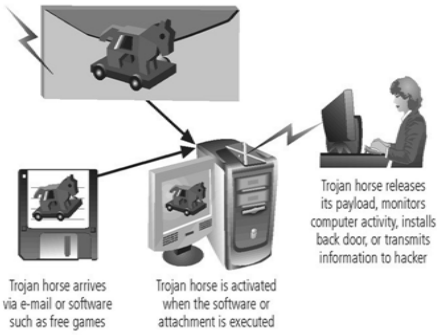

Figure 5 : Trojan horse

Chernobyl virus- It deletes all Microsoft Office saved files and it deletes partition information from the disk that causes a big loss of data. The Chernobyl virus damage most of the central computer system. Only a computer or system technician can fix this through physical struggles.

Risk of Attacks

I. Unauthorized access from external or internal users.
ii. Loss from a hardware or software failure.
iii. Unreachability because of network failure.

Risk Category

i. Damage- Result in data physically lost.
ii. Disclosure- Leaking critical information.
iii. Losses- This might be temporary or might be permanent.

Risk Factors
i. Physical Damage
ii. Malfunctions
iii. Attacks
iv. Application errors
v. Human errors

3. Denial of Service Attack (Dos)

Attacker sends a huge number of different links or information request to a targeted system. The targeted system cannot handle well real service along with others. For example UDP flooding and SYN flooding shown in fig.6

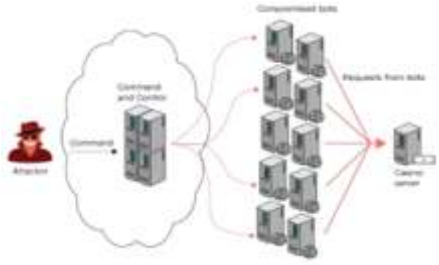

Figure 6 : DoS

4. Distributed Denial of Service Attack

Distributed denial of service attack appears when several systems flood the bandwidth or resources of the selected system generally more than one web servers. For example, botnet flood target system with traffic as shown in Fig.6.

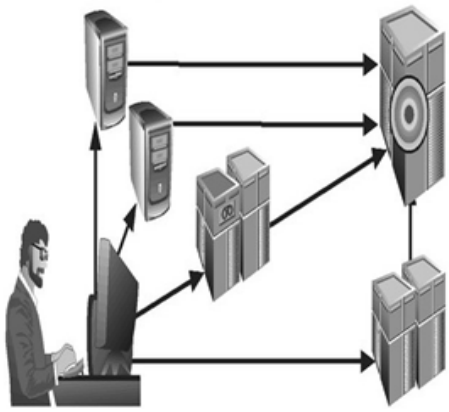

Figure 7 : DoS vs DDoS Attack

Spam- is the electronic junk e-mail. It contains transfer unwanted message, often-unwanted advertisement. It is used for purpose of delivering the worms, Trojan horse, viruses, targeted phishing attack or spyware. For example

Unwanted and meaningless messages with virus blocked by some antivirus solutions.

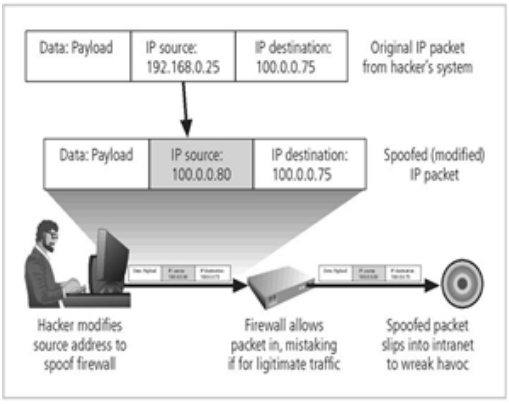

Figure 8 : Spoofing

In Fig.8. The graph shows some techniques that used to gain unapproved access intruder assumes a confidential IP address.

Man in the Middle Attack

Attacker display networks packets modify them and insert them back into the network.

For example

- Computer 1 attempt to establish encoded session with company 2.
- Company 2 send all message to a hacker who receive, copies, decrypt, and forward a copy to company 2.
- The hackers interrupt transmission and positions as company 2. The hacker's give-and-take his own keys with the company 1. Hacker then creates a session with company 2, present as company 1.

Packet Sniffer

A packet sniffer is application software that use the network adapter card to catch all network packets that are sent through a LAN.

Computer Security

Different companies and organizations have a different style of action. This statement spread to the ways they set up their computer network or systems and operating techniques. That creates it difficult for any document to fix down detail set of processes that can be used to cover every company or every organization.

Virus preventions

- The ways in which virus prevention did are:
- Services Patching
- Operating system patching
- Password
- Antivirus software
- Patching the client software
- Firewalls

Virus Detection

Primary step of detection of antivirus is check program or file in the system for virus signature. However, best antivirus uses many methods to find or search the system for viruses.
Antivirus consideration: During selecting or choosing antivirus software, the following steps could be considered:

- Per work station or server cost
- Updates frequency
- Ease of updates installation
- Certification

Antivirus software that mostly used are:

1. Alwil software
2. AVG antivirus
3. Central command
4. Computer Associates
5. Dr. Solomon's software
6. Aladdin knowledge
7. Command software
8. Data fellow corp.
9. ESET software
10. Finjan software

Clean Viruses- Clean virus based on your antivirus solution. The threat recognized before cleaned, so it creates sense to try antivirus software scanner at first. If software recognizes but cannot remove or clean the virus, checked the manufacturer website for manual instruction removal.

Perform basic safety and security maintenance – Use internet 'firewall', and use the up to date antivirus software, & update your computer system.

A. Use Firewall

Firewall is hardware or software that makes a protective wall between computer & possibly damage content on the network or on the internet. The firewall is very helpful to guard your pc against harmful or malicious users or from computer viruses, worms, also from malicious software.
B. Update Computer From the internet downloads a service pack and update. As shown in Fig. 9.

Figure 9 : Update your Pc

CONCLUSION

There are several and many viruses in the world and every day new viruses are coming up. In addition, there are new antivirus programs, software, and techniques coming up too. It is good to be a little worried or suspicious about

malware when you are surfing on the internet or also download files. Be aware of new viruses or infections out there. Take the best precautions methods and backup your data always. Always keep up to date computer security software, antivirus, or window firewalls software. Avoid the files or program from unknown sources. I think we should not use the computer system without any antivirus security as it may harm or damage to our personal important data. Make sure do not transfer or copy any file or data without scanning the disk.

References

[1] B. K. Mishra and D. Saini, "Mathematical models on computer viruses," Appl. Math. Comput., vol. 187, no. 2, pp. 929-936, 2007.

[2] J. R. C. Piqueira and V. O. Araujo, "A modified epidemiological model for computer viruses," Appl. Math. Comput., vol. 213, no. 2, pp. 355-360, 2009.

[3] V. Tasril, M. B. Ginting, and A. Mardiana, "Threats of Computer System and its Prevention," Int. J. Sci. Res. Sci. Technol., vol. 3, no. 6, pp. 448-451, 2017.

[4] Q. Zhu, X. Yang, L.-X. Yang, and X. Zhang, "A mixing propagation model of computer viruses and countermeasures," Nonlinear Dyn., vol. 73, no. 3, pp. 1433-1441, 2013.

[5] J. R. C. Piqueira, A. A. De Vasconcelos, C. E. C. J. Gabriel, and V. O. Araujo, "Dynamic models for computer viruses," Comput. Secur., vol. 27, no. 7-8, pp. 355-359, 2008.

[6] D. Shah and T. Zaman, "Detecting sources of computer viruses in networks: theory and experiment," in ACM SIGMETRICS Performance Evaluation Review, 2010, vol. 38, no. 1, pp. 203-214.

[7] C. Nachenberg, "Heuristic detection of computer viruses." Google Patents, 2009.

[8] J. Ren and Y. Xu, "A compartmental model for computer virus propagation with kill signals," Phys. A Stat. Mech. its Appl., vol. 486, pp. 446-454, 2017.

[9] L.-X. Yang and X. Yang, "The effect of network topology on the spread of computer viruses: a modeling study," Int. J. Comput. Math., vol. 94, no. 8, pp. 1591-1608, 2017.

[10] M. R. Parsaei, R. Javidan, N. S. Kargar, and H. S. Nik, "On the global stability of an epidemic model of computer viruses," Theory Biosci., vol. 136, no. 3-4, pp. 169-178, 2017.

[11] R. K. Upadhyay, S. Kumari, and A. K. Misra, "Modeling the virus dynamics in a computer network with SVEIR model and nonlinear incident rate," J. Appl. Math. Comput., vol. 54, no. 1-2, pp. 485-509, 2017.

[12] D. Ferbrache, A pathology of computer viruses. Springer Science & Business Media, 2012.

[13] J. Parikka, Digital contagions: A media archaeology of computer viruses, vol. 44. Peter Lang, 2007.