ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 2, Issue 4 (Oct. - Dec. 2014)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)

Network Security- Virus Attacks and Defence using Antivirus Software

Trupti Shah
Research Scholar of JJT-University, Rajasthan, India

Abstract
Network security is important in every field of today's world such as government offices, educational institutions, any business organization etc. So data security is the extreme critical factor in ensuring the safe transmission of information through the network. Threats to data privacy are powerful tools in the hands of attackers that could use the vulnerabilities of a network to corrupt, destroy and steal the sensitive information. There are many network security measures to protect the data from the hands of the attackers like antivirus software, firewalls, cryptography etc. In this paper an attempt has been made to study different viruses which can harm the computer. It outlines about antivirus software which can detect viruses; worms etc. and warn the user of their presence in computer and deactivate then clean up the computer of malicious software.

Keywords
Vulnerabilities, Threats, Network Security Measures, Antivirus Software, Firewalls and cryptography.

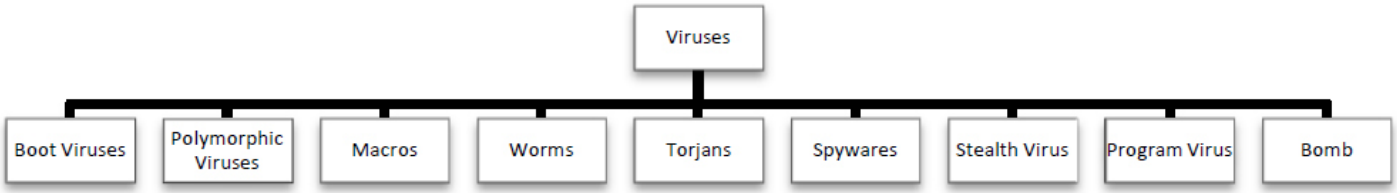
I. Introduction

Now-a-days, there are so many unethical practices in the form of digital attacks which are causing problems in the field of Information Technology. These attacks are sometimes in the form of malicious software which enter in the system by themself without the knowledge of the user and sometimes in the form of an unauthorized user who get the access to computer system for the purpose of damaging the stored data, to steal information or to keep the eyes on a user's activity. Some of the common forms of the digital attacks are: Computer Virus, Spams, Phishing, Spyware, Adware, Hacking, Cracking, etc. These threats are primarily present due to the ignorance shown by the users, weak technology and poor design of the network. To protect data from such network viruses' one of the network security measures is antivirus software. When considering network security, it must be emphasized that the whole network is secure. Network security does not only concern the security in the computers at each end of the communication chain but also when transmitting data on the communication channel. Here are some common digital threats to computers.

II. Digital Threats

Virus (Vital Information Resource Under Siege): Computer viruses are the malicious programs having the ability to replicate and execute themselves. They can attach themselves to the other program, files or data stored in the system automatically without any instructions from the user. It can enter in a computer by different means like when one copy some data from the virus infected system to another uninfected system or while downloading some programs from the Internet or it can come to system as an e-mail message. A computer virus spreads itself from one computer to another and interferences with the normal operations of a computer. Viruses attach themselves to any type of executable and system files, causing the unusual behavior of the programs or sometimes causing the system crash. Different Types of viruses are shown in the following chart1. Based upon their working behavior, target infection computer viruses can be categorized as below.

Chart 1: Different Types of Viruses



(i) Boot Viruses: These types of virus infect the Master Boot Record (MBR) of the hard disk drive or DOS Boot Record (DBR) of the CD. Every time a system is booted with an infected hard disc, these viruses become active and start infecting the stored data. Danish boot, PC stone, Joshi, brain, Empire, Azusa, Michelangelo, etc. are the examples of boot viruses. Crazy Boot is a computer virus that infects the Microsoft Windows operating systems.

(ii) Polymorphic Virus: A virus that changes its virus signature (i.e., its binary pattern) every time it replicates and infects a new file in order to keep from being detected by an antivirus program. A polymorphic virus is one that creates copies of itself, with variations in each copy to fool a virus detection program and user. The variations are typically different encryption methods in the virus file copies, which makes it more difficult for a virus detection program to detect and remove a polymorphic virus from a computer.

(iii) Macros: The main target area of these viruses is to infect the data file of the system like MS-Word, MS-Excel files etc. These types of the viruses destroy the data stored in the system causing irrecoverable damage sometimes. They can spread from one computer to another on the network or through internet, as most of the time data files are transferred from one system to another. Melissa, WM.concept.A, Bloodhound, etc. are the examples of macro virus.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

(iv) Worm: A worm is a computer program that uses computer networks to send copies of itself to other computers on a network. A virus requires human action such as transferring of an infected file to spread itself. A worm can spread without any human action too. It replicates itself without the knowledge of the user. Worms can cause severe harm to a computer network as blocking the network and reducing the speed of the network. They reduce the storage space and available memory of the system. There are two main types of worms, mass□mailing worms and network□aware worms. Mass mailing worms use email as a means to infect other computers. Network□aware worms are a major problem for the Internet. A network□aware worm selects a target and once the worm accesses the target host, it can infect it by means of a Trojan or otherwise. Scalper, Swen, Morris worms and Mydoom are the examples of the worms.

(v) Torjan Horse: A computer program that appears to be useful software but actually causes damage once installed or executed on the computer system is known as a Torjan horse. After getting installed, it allows unauthorized access to the computer. Torjan effects are very dangerous as they allow the computer to be remotely controlled by someone else and can cause loss of the personal and confidential information. They are not self-replicating and the only way, they can spread is copying to the other system, e.g. Zeus, Beast, Back Orifice, The Blackhole Exploit Kit etc.

(vi) Spywares: It stores personal information and surfing details and send them to its website without informing the user. Many spywares get installed automatically as a free download while installing software.

(vii) Stealth Virus: these types of viruses are capable of changing their appearance by changing their codes. This way, they can hide their existence from the Antivirus programs. Sometimes, it hides the increased size of the file due to virus infection causing the file to be scanned as an uninfected file. Frodo, Brain are the example of Stealth viruses.

(viii) Program Virus: It also known as the Parasitic viruses, they infect the program files of the system having extensionas.com, .exe, .sys, .ovl, .dll, .Scr etc. These viruses do not affect the boot records of the system. Program files are their attractive targets, because these files are used very frequently and moreover the format of these files is quite simple. So when these programs are used they become active in the computer's memory and start their destruction work.

(ix) Bomb: These types of viruses remain inactive and undeleted in the system for a long time and wait for a specific event or date to trigger. Viruses that active on certain dates are often called time bomb. For example, Jerusalem –B or Israeli Virus or Friday 13th Virus waits for Friday the 13th and deletes the program files executed on that day.

Thus Viruses, worms and Torjan Horse may harm the data or affect the performance and the speed of the computer.

Data Theft: It is a very serious problem for computer networks. People break into computer networks to either disrupt their functioning or to steal confidential information. Hackers are the computer experts who can break into the computer systems and networks. There are two types of hackers – white hackers and black hackers. White hackers study and break into networks to find and fix security loopholes. They offer their services to corporations, public organizations and educational institutions to make their networks more secure. Black hackers or crackers have a criminal intention. Some examples are cracking confidential information like results of the students in any educational institutions and attacking the computer network of any organization.

III. Defense Mechanism Against Viruses

Threats will continue to be a major issue in the global world as long as data is accessible and transferred across the network. So, it better to take the prevention measures to safeguard the system from any type of virus attacks. Different defense mechanisms are developed to deal with these attacks.

(i) Avoid the use of external or unknown storage devices and if required, scan them properly with some good Antivirus software.
(ii) While working with emails do not open the unknown mails.
(iii) Before downloading any file or program from the internet, make it sure that the source is reliable one.
(iv) Never install the pirated software.
(v) Install effective Antivirus software in the system and update it periodically.
(v) If the computers are connected to the network, restrict the access of the computer and allow only to the genuine users to use the system resources.
(vi) Always keep a backup copy of the data.
(vii) Develop a virus prevention plan – install network based Antivirus, and educate the network users.

Anti-Malware Software and scanners: Viruses, worms and Trojan horses are all examples of malicious software, or Malware for short. Special so-called anti-Malware tools are used to detect them and cure an infected system. Every computer on a network must have antivirus software. Installed in it and it should be updated on a regular basis. Antivirus software can be used to protect the computer from various types of malware. Antivirus software can detect viruses; worms etc. and warn the user of their presence in the computer. It can also deactivate and clean up the computer of malicious software. These are the memory resident programs and get activated as soon as the system is started. It checks all the files in the system and incase any virus is detected, it removes it. Also while working on the computer, if some infected storage device is used, it generates the warning messages and stops the data transfer. Some of the Antivirus softwares are: Norton, AVG, Quick Heal, McAfee, PC-cillin etc.

IV. Conclusion

When new viruses are found virus definitions are updated. Currently research is being focused on neural networks for facial recognition software. Most current algorithms require substantial processing power. This power cannot be available in small devices like sensors. Therefore, one must develop light weight algorithms to counter this problem [1]. Antivirus works on a very basic principle; they scan a file and then matches its digital signature against the known malwares. If the signature is match in the database it reports it, delete it or even disinfect it depending on the user's setting. This system however easy has a huge drawback, whenever a new malware is found; it takes time before the antivirus database can be updated and during this period the malware can already take complete control of the computer, disables the antivirus or even hides itself from the antivirus. To prevent this antivirus companies introduced a new system called cloud scanning these ways not only will the digital signature be scanned across the database but also across millions of computers and servers across the world. This all happens and real time and results are very fast. This greatly reduces the chance of infection

from a new malware.

V. References

[1]. *Anupriya Shrivastava, M A Rizvi, "Network Security Analysis Based on Authentication Techniques", International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 3, Issue. 6, June 2014, pg.11 – 18 Bhavya Daya, "Network Security: History, Importance, and Future", University of Florida Department of Electrical and Computer Engineering*

[2]. *B. Daya ,"Network Security: History, Importance, and Future ,"University of Florida Department of Electrical and Computer Engineering , 2013. Kartikey Agarwal, Dr. Sanjay Kumar Dubey Amity University, Noida, Uttar Pradesh, India," Network Security: Attacks and*

[3]. *Defence" International Journal of Advance Foundation and Research in Science & Engineering (IJAFRSE) Volume 1, Issue 3, August 2014.*

[4]. *Mayuri V. Chaudhari, "QUANTUM CRYPTOGRAPHY: AN EMERGING TREND IN NETWORK SECURITY", IEEE Sponsored International Conference On Empowering Emerging Trends In Computer, Information Technology & Bioinformatics*

[5]. *International Journal of Computer, Information Technology & Bioinformatics (IJCITB) ISSN: 2278-7593, Volume-2, Issue-2*