A Review Paper on Cyber Security

Saloni Khurana
Department of Electronics & Communication
Vivekananda Institute of Technology, Jaipur
Jaipur, India

Abstract: **We will be analyzing a variety of cyber-attacks and different security methods. We aspire to create research into the subject area. This paper explores how cybercrime has become a serious threat in our lives and we are going to look at a few of the different security methods that are being used in this arena and their various weaknesses.**

INTRODUCTION

Cyber security is generally the techniques set to protect the cyber environment of the user. This environment includes the user themselves, the devices, networks, applications, all software's etc.

The main objective is to reduce the risk including cyber attacks.

Cyber security is the branch of computer security related to internet. The main security objective is to project the device using various rules and to establish various measures against attack over the internet.

There are various methods that are used to prevent online attacks and enhance internet security. With the rise of online activities, applications the cyber-attacks are increasing day by day.

THREATS

- MALICIOUS SOFTWARE

A computer user can be forced sometimes to download a software onto a computer that is of malicious intent. Such software comes in many forms, such as viruses, Trojan horses, and worms.

1. VIRUS

It is the type of malicious software that, when executed replicates itself by modifying other computer programs. Computer viruses causes economic damage due to system failure, corrupting data, increasing maintenance cost etc.

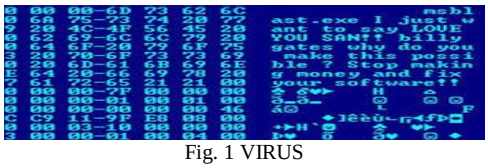

Fig. 1 VIRUS

1. WORMS

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computer. Many worms are designed only to spread, and do not attempt to change the systems they pass through.

Fig. 2 WORMS

2. TROJAN HORSE

A TROJAN HORSE, commonly known as a Trojan , is a name for malicious software that tends to be harmless, so that a user by will allows it to be downloaded onto the computer.

Trojan allow an attacker to hack users' personal information such as banking information, email passwords, personal identity. It also affects other devices connected to the network.

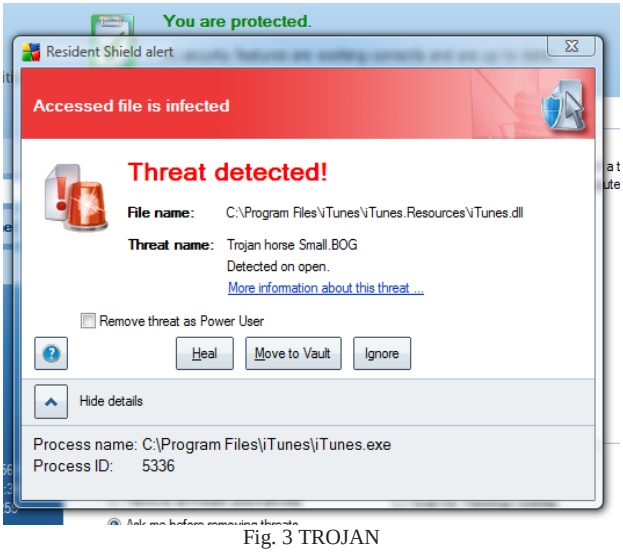

Fig. 3 TROJAN

3. MALWARE

MALWARE is a term short for malicious software, used to destroy computer operation, gather very sensitive information, or gain access to private computer systems. Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm due to some deficiency. The term malware is sometimes used for bad malware and unintentionally harmful software.

- *PHISHING*

It is the attempt to obtain sensitive information such as credit card details, usernames, passwords etc. often for the malicious reasons.

Phishing is typically carried out by the instant messaging or email spoofing and it often directs users to enter personal details at a fake website. Phishing emails may contain links to website that are infected with malware.

Phishing is the main example of social engineering techniques used to deceive users and exploits weakness in current web security.

Phishing is of different types-

SPEAR PHISHING

Phishing attacks directed at any individual or companies have been termed as spear phishing. This is the most successful technique on the internet today with 91% of attacks.

In this the attackers gathers the information about the companies and their targets to increase their probability of success.

Clone Phishing

It is the type of phishing attack where an email containing an attachment or link has had its content and recipient address (es) taken and used to create an almost identical or cloned email.

Whaling

Several phishing attacks have been directed specifically at senior executives and other people with high-profile targets within businesses so these types of attacks are termed as whaling.

- KEYSTROKE LOGGING

It is often referred as key logging or keyboard capturing in which the person using the keyboard is unaware of the fact that their actions are being monitored. It is basically the action of recording the keys struck on the keyboard.

There are various key logging methods ranging from software and hardware based approaches to acoustic analysis.

1. *Software Based Key Loggers*

These are computer programs designed to work on the target computer's software. Key loggers are used in IT firms to troubleshoot technical problems with computers and business networks. Families and business people use key loggers legally to monitor network usage without their users' knowledge.

1. *Hardware Based Key loggers*

Hardware-based key loggers do not depend upon any software being installed as they exist at a hardware level in a computer system.

REMEDIES

- FIREWALL

A computer firewall controls the access between the networks. It contains filters depending upon one firewall or the other. Firewall is basically a computer security system that controls and monitors the incoming outgoing network traffic based on security rules. A firewall basically establishes a barrier between a trusted, secure internet network and other outside network such as internet that is not considered as secured or trusted.

- INTERNET SECURITY PRODUCTS

1. ANTIVIRUS

Antivirus software and internet security programs are able to project a programmable device from attack by detecting and eliminating the viruses. Antivirus software was used in the early years of internet but now with the development several free security applications are available on internet.

2. PASSWORD MANAGERS

The password managers is a software application that is used to store and organize the passwords. Password managers usually store passwords encrypted, requiring the person to create a master password; a single, ideally a very strong password which allows the user access to their entire password database.

3. ECURITY SUITS

The security suits contains the suits of firewalls, anti-virus, anti-spyware and many more. They also gives the theft protection, portable storage device safety check, private internet browsing or make security related decisions and are free of charge.

- SECURITY TOKENS

Some online sites offers the users the ability to use the six digit code which randomly changes after every 30-60 seconds on a security token. The keys on the token have built computations and manipulated numbers based on the current time built into the device. This means that after every thirty seconds there is only a certain sequence of numbers possible which would be correct to access to the online account.

CONCLUSION

This paper is basically trying to tell about the various cyber-attacks and the various security methods that can used to prevent our device from getting attacked. Also it helps to overcome several loopholes on their computer operation.

REFERENCE

[1] https://en.wikipedia.org/wiki/Phishing
[2] https://en.wikipedia.org/wiki/Internet_security#Phishing
[3] https://en.wikipedia.org/wiki/Malware