PRAJÑĀ - **Journal of Pure and Applied Sciences Vol. 24 – 25 : 219 – 222 (2017)**
ISSN 0975 - 2595

CYBER SECURITY: ATTACKS AND ITS COUNTERMEASURES

PRASHANT P. PITTALIA

Department Of Computer Science, Sardar Patel University, Vallabh Vidyanagar-388120, Gujarat, India
E-mail:prashantppittalia@yahoo.com

ABSTRACT

The Internet is growing rapidly. It has given rise to new opportunity in every field like – business, financial institution, education, health, sports, entertainment, government, defense, power sector, etc. It has removed the geographical boundaries between the users and allowed the Internet users to access the information or resources from any place by sitting only on the single place. The biggest drawbacks of the Internet is cyber crime, which is an illegal activity performed by the users using the Internet. Cyber crime involves breakdown of the privacy of a system, damages files and folders, involves unethical hacking of the credential information, identifies the loopholes in the website and misuses for malicious task. In today era, most of the cyber crimes are committed by the people who have knowledge of a technology. To remove such malicious activities, it is necessary to understand their activities and apply the proper prevention strategies. Organizations or persons who use the Internet have a lack of responsibilities of online resources and allow the cyber attacker to breach the security. This paper provides a current scenario of cybercrime and proper prevention steps.

Keywords: Cyber crime, hacking, port scanning, ransomware, firewall

INTRODUCTION

In today's IT environment, the Internet and computer network is very important and useful part of daily work. The people are doing most of their work like selling, purchasing, payment of goods, storing their important contents, sharing their useful and secret information. Today internet is become a part of human lives. The growing fastest world of internet is known as cyber world. Today cyber security is most important in the Internet world.

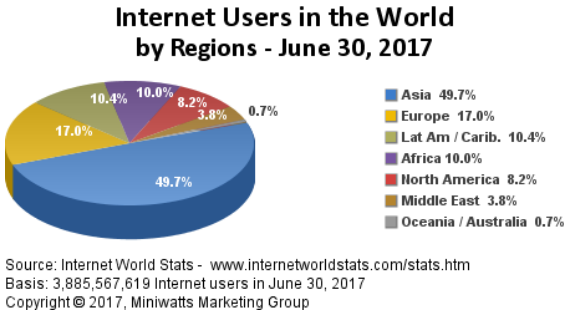

Fig: 1. Internet Users in the world by Regions – June 30, 3017 [1]

Asia is the continent having 49.7% of the Internet users in the world. It shows that most of the users on Internet are from Asia. It shows that more number of users spare their time on Internet for doing their online activities like social media, online transactions, surfing the net and transfer different types of files.

CYBER ATTACKS

Attackers are typically trying to attack or manipulate one or more networks to achieve their objective. The Internet was designed for utility and robustness. Cyber criminals use internet and computer technology to hack user's personal computers, laptops, mobile phone's data, and credential details from social media, business websites, national secrets etc. Criminals who perform these illegal activities through the internet are called – Hackers. The majority of cyber crimes are as follow.

Phishing

In this type of crime hackers provides a link which redirects to the fake website which is looks and feel like same as the legitimate one. Users are move to that fake sites and gives his/her credential information, which steal by the attacker and misuse or sell to the others. In such attacks the URL are similar to the original websites only few characters are changed or the name should be as it is but the domain name should be change. Most of phishing attacks are done by sending an email to the people and provide their credential information. [3]

Malicious Code

It is a code that damages a computer or system. It could not be identified by the antivirus software. Virus, worms, Trojan horse, java attack applets, ActiveX control are the various types of code which may be attached with the application or attachment to harmful the system or computer. Attackers identify the weakness of the operating systems or the application by testing various new malicious codes on such software and then such tested malicious code is spread across Internet.

Defacement

Website defacement means changes the content of a website by attacker by cracking the security of a website owner. Such type of attacker targets some government agencies of other countries and shows their strength by identifying weaknesses in their website.

Spam

It is the use of electronic messaging systems to send unwanted messages, especially advertising, as well as sending messages repeatedly on the same website.

Network Scanning

It is used to identify the network of an organization by knowing the IP addresses in the network, operating systems and applications running on the system, port numbers used to access the particular application. Also it identifies which port numbers are live and what applications are running on it and find out the weaknesses of it to perform the malicious task. Standard operating systems and software having predefined services running on predefined port numbers. Also it has pre-configured the some default usernames and passwords, which leads to easy task of the attacker to scan such port numbers using such data. [5]

Hacking:

In Internet world most dangerous cyber crime is hacking. Hacking simply refers to the breaking into the computer system and steals valuable information from the system without any permission. Hacking is done by hackers who run the client or server program and able to spoof the data.

Fake Certificates and Certificate Authorities

On internet trustworthy websites are identify by seeing the HTTPS (Secure Hyper Text Transfer Protocol) at the address bar in the web browser. The CA (Certificate Authority) verify the identity of a requester and if it is valid than issue a signed certificate which mention the purpose of the website and validity of the certificate. Every browser comes with a copy of CA's signatures so that when user tries to access the website it is trustworthy or not is easily identify. If CA's of signed certificate on a website is not trusted by a web browser, it will warn the users about it.

Attackers target these trusted CAs and try to get fake certificate IDs signed by the CA to make them as original. Then when a victim connects to the website a legitimate certificate send bypassing the inbuilt security and web browser could not provide warning to the users.

Identity theft:

In identity theft, the attacker use someone else identity to misuse and on behalf of actual user it fraud with others. In such attack it theft money or getting benefits by pretending to someone else. Without permission use someone else electronic signature, unique identification features like password is known as identity theft.

CYBERSPACE & CYBERCRIME

With rapid growth of the Internet also increase incidents of online attacks. In 2017, ransomware attacks like "WannaCry" and "Petya" spreading around the world and demanding for bit coins. According to analysts with IT-security software firm G Data, in 2017 the number of new malware specimen is more than 7.4 million.

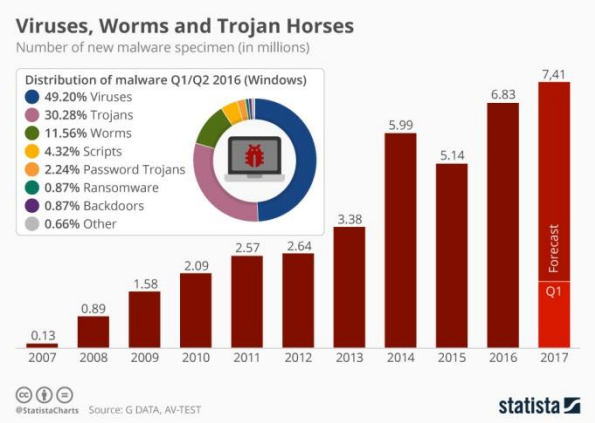

Fig: 2. Number of new malware specimen (in millions) and the share of windows-based malware (in percent) [2]

CYBER SECURITY: PREVENTION STEPS

Today the cybercrime is the major threat for the development of any state or country. Cyber criminals wants to get money, destroy the systems, or harassment someone. It is necessary to implement the cyber crime prevention techniques in very well manner. It is needed to awareness internet users about the cyber threats and how to secure their credential information. Internet users should be aware about the security tools to reduce the risk of cyber crime. The following steps are important to prevent the system against the malicious activity on a system.

Use Strong Passwords:

Use the different password and username combinations for various accounts and instead of write it down on paper keep it in your mind.

Make Social Media Account Safe:

Be sure to keep your social networking profiles (Face book, Twitter, YouTube, etc.) private. Be sure to check your security settings. Think twice before making someone as a member of your group and careful of what information you post online and whom you allow to access it.

Secure your Mobile Devices:

Mobile devices are also vulnerable to malicious software, such as computer viruses and cyber attackers. Always download applications from trusted sources. It is also important to update operating system time-to-time. Install standard anti-virus and firewalls. Also set the pattern matching or biometric authentication, otherwise, anyone can access all your personal information, if you misplace it or even set it down for a few moments. Someone could install malicious software that uses your GPS and track about your movement. Do not hurry to download the apps or games on your device. Before download check the permissions that should be demands by the application.

Protect your data:

Credential information like (financial records, credit card and debit card details, tax related information) should be stored with strong cryptographic algorithms that supports authentication, confidentiality and integrity of the data.

Keep your device with latest patches and updates:

Every operating systems and applications are releasing the new version with latest updated information to more secure their software. Regularly update your device with patches when they become available. It helps to block attackers from being able to take advantage of software vulnerabilities that they could otherwise use to crack your system.

Install security software:

Security software essentials like firewall and antivirus programs. Firewall controls who can communicate with your computer system online & what information is allowed to access. It continuous watches all the data attempting to flow in and out of your computer on the Internet, allowing communications that it knows are safe and blocking “bad” traffic such as attacks from ever reaching your computer. It checks your

current connections and according to it allows only those packets which belong to those connections to and from your computers. Proper configuration of firewall on a system is very essential to protect from outsider attacks. [4]

Choose the right person for help:

If you are victim of any type of cyber attacks do not be hesitate, If you come across illegal online content, or if you suspect a cybercrime, identity theft or a commercial scam, just like any other crime report this to your nearest police station.

CONCLUSION

Today's Internet websites are mostly utilized for the sales, marketing of products, services of an organization, financial institutions, government projects & social networking etc. It can be used for knowledge, research, online transactions, fun and maintain relationship with people. There is a vast amount of credential information stored on various websites, and the lack of proper security makes these applications an ideal sandbox for attackers. Such websites can place an individual or a company in a compromising position or at serious risk. Peoples needs to understand what is secret and what to share online and to whom, otherwise it will harmful for the user or organization.

REFERENCES

[1] Internet world stats:http://www.internetworldstats.com / stats.htm

[2] Statista - The portal for statistics: https://www.statista.com/chart/10045/new-malware-specimen-and-share-of-windows-based-malware/

[3]Computer Hope: https://www.computerhope.com/jargon/c/compcrim.htm

[4]Digital care solutions: https://www.digitalcare.org/cybercrime-prevention-tips/

[5] Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Nina Godbole and Sunit Belpure, Publication Wiley