IJCSMA

Pallavi Rane, International Journal of Computer Science and Mobile Applications,
Vol.5 Issue. 8, August- 2017, pg. 68-75 **ISSN: 2321-8363**
Impact Factor: 4.123

Types of Cyber Crimes and Prevention Measures

Pallavi Rane

Assistant Professor, Department of Computer Science, M.J. College Jalgaon, Maharashtra, India

Abstract: The increased use of internet can easily gives access to huge information in a few seconds. This gives rise to cyber crimes. Cyber -crime is a crime committed by internet and technocrats. This Paper discusses with Variants of cyber crime like terrorist attack, cyber extortion, crimes against individuals, crimes against property, and crimes against organization. It also includes impact on the real world and society, and how to handle cyber crimes.

Keywords: Types of cyber Crime, prevention measures of cyber crimes

I. INTRODUCTION

In today‘s world, an association dependence on cyberspace is becoming an progressively more important aspect of administrative security. The framework of different associations are interrelated in cyberspace, therefore the level of risk to safety has increased theatrically. As colleges and Universities stores same record as bank, Computer systems at these places are main targets. The Use of computer, internet, cyberspace and the World Wide Web gives rise to cyber and the criminal activities. Cyber criminals are becoming more refined and are targeting customers as well as public and private officialdoms. Cyber crimes are risen due to the cyber security illiteracy.

The computer and the person behind it as victims leads to cyber crimes. Cyber crime includes anything such as downloading Illegal music files to stealing cash from online bank accounts, creating duplicate CD's of software. Cyber crime could also creating and distributing small or large programs written by programmers called viruses on other computers or posting confidential business information on the Internet to harm the peoples. An important form of cyber crime is identity theft, in which criminals use the Internet to steal personal information from other users.

It can be classified as : Spamming, Stalking, Extortion, Blackmail, Bullying, Phishing, Hacking, Malware ,Exploiting vulnerabilities, Social Engineering and Identity Theft (Fake emails, fake phone conversions using data obtained from Internet, to get more information about you and your bank, cards, etc.)

Cyber-crime usually involves the following:

Unauthorized access of the computers, Data diddling, Virus/worms attack, Theft of computer system, Hacking, Denial of attacks, Logic bombs, Trojan attacks, Internet time theft, Web jacking, Email bombing, Salami attacks, Physically damaging computer system.

Here are the examples of cyber crimes that were happened in 2016

1. **Ransomware emerges as a top cyber threat to business**

In May 2016, Security researchers at Kaspersky Lab and FireEye confirmed that the upward trend of ransomware was continuing and had emerged as a top threat to business.

This was confirmed by Eset data which showed that ransomware made up a quarter of UK cyber attacks, and was continuing to rise, while in August Trend Micro reported that the occurrence of ransomware families nearly doubled in the first half of 2016 compared with the whole of 2015 and PhishMe research concluded that ransomware is a mature business model for cyber criminals.

The impact of ransomware was underlined by a study, also published in August, that found that one in five businesses hit by ransomware are forced to close, but despite this harsh reality, another study found that almost two-thirds of US office workers were unaware of ransomware threat, emphasising the need for cyber security awareness training.

2. **UK second only to US in DDoS attacks**

The UK is second only to the US in being targeted by distributed denial of service (DDoS) attacks with the aim of vandalism, disrupting businesses or extorting money from businesses, a report revealed in August.

Although DDoS mitigation technologies are fairly mature, security consultants report that after ransomware attacks, DDoS attacks were the most common reason for callouts from affected businesses in 2016. DDoS attacks are not new, but attackers have been exploring new techniques for delivering more powerful attacks over longer periods. DDoS attacks have also been driven by the release of the Mirai code for establishing IoT botnetsand the availability of DDoS services for as little as $5 an hour.

3. **412 million user accounts exposed in FriendFinder Networks hack**

In the biggest data breach of the year, user details of more than 412 million accounts were exposed in a data breach at FriendFinder Networks, that once again confirmed poor user data protection and poor password practices.

In addition to confirmation of a 2014 breach at Yahoo that exposed a record 500 million accounts, 2016 also saw a string of other breaches, including the Dailymotion breach, which prompted calls for password alternatives, the US Navy breach, which highlighted third-party cyber risk, the breach at mobile network operator Three, which highlighted several security issues, the Dropbox breach, and the Australian Red Cross Blood Service data breach, which showed security is still not a priority for many organizations.

4. **Financial Conduct Authority concerned about cyber security of banks**

The Tesco Bank heist also led to the UK’s Financial Conduct Authority (FCA) expressing concern about weaknesses in banks’ IT systems, which also emerged as a theme in 2016.

In October, the US Treasury called on banks to provide more cyber attack information after the attempted $1bn bank heist in which cyber criminals still managed to get away with $81m, which Swift said highlighted the gap between attacker and defenders. Swift also warns banks of fresh wave of cyber heists as security researchers reported financial cyber attacks were increasing as malware writers were join forces after cyber attacks on at least three Asian banks were found to share malware links

5. **Industrialized cyber crime disrupting business, report reveals**

Despite the evidence that much cyber criminal activity is carried out by professional cyber crime organisations, many businesses are ill-equipped to deal with the threats posed by profit-oriented and highly organised cyber criminal enterprises, a BT-KPMG report revealed in July.

II. Reasons for cybercrime

Hart in his work " The Concept of Law" said that 'human beings are vulnerable so rule of law is required to protect them'. By applying this to the cyberspace we may say that computers are vulnerable so rule of law is required to protect and safeguard them against cyber crime. The reasons for the vulnerability of computers may be said to be:

1. Capacity to store data in comparatively small space:-

The computer has a unique characteristic of storing data in a very small space. This allows for much easier access or removal of information through either physical or virtual media.

2. Easy to access:-

The problems encountered in guarding a computer system from unauthorised access are that there is every possibility of unauthorised access not due to human error but due to the complex technology. By secretly implanted a logic bomb, key loggers that can steal access codes, advanced voice recorders; retina imagers etc. that can fool biometric systems and bypass firewalls can be utilised to get past many security systems.

3. Complex-

The computers work on operating systems and these operating systems in turn are composed of millions of lines of code. The human mind is fallible and it is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the computer system using often more sophisticated means than originally anticipated by the systems engineers.

4. Negligence:-

Negligence is very closely connected with human conduct. It is therefore very probable that while protecting the computer system there might be any negligence, which in turn provides a cyber criminal to gain access and control over the computer system. This negligence is usually a property of under resourced IT security provisions and the improvement of security barriers within software packages and network structures could lead to improved security.

5. Loss of evidence:-

Loss of evidence is a very common & obvious problem as all the data is routinely destroyed. Further collection of data outside the territorial extent also paralyses this system of crime investigation.

III. Different Types of Cyber Attack

Attacks Comes in 2 states as Active attacks and Passive attacks. During an active attack, the criminal tries to modify a system's data, assets or processes. However, a passive attack simply includes access to the system/device and usage of computer system's information – without trying to alter its resources, operations or data.

1) Cybercrime alongside with individual

i. E-Mail Spoofing**:** this means a spoofed email is one that seems to initiate from one source but actually has been sent from another source. This can also be named as E-Mail forging. The main goal of the attacker/enemy is to disturb the victim's e-mail service by sending him a large number of emails.

ii. Phishing: It is a way of fraud in which the attacker tries to learn information such as login identifications or account information by checking as a reputable entity or person in email or other communication channels.

iii. Spamming: Spam is the misuse of electronic messaging system to send spontaneous bulk messages comprehensively.

iv. Cyber defamation/insult: It involves any person with intent to lower down the dignity/image of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.

v. Cyber stalking and harassment: This annoyance could be sexual in nature, or it could have other stimuli including anger.

vi. Computer disruption: the use of the internet to stop the normal functioning of a computer system through the introduction of worms, viruses, or logic bomb is referred to as computer disruption.

vii. Malicious Code

viii. A set of instructions that is get installed on your device and performs some unauthorized activities is malicious code. This set of instructions is referred as Malware or malicious software which is created to damage the device/network, with the help of viruses, Trojan horses and other harmful programs.

2) Crime against belongings

i. Intellectual Property Crimes**:** The most common type of crimes are software piracy, infringement of copyright, trademark , theft of computer source code, etc.

ii. Cyber Bending**:** When two persons appealing for the same Domain Name either by claiming that they had registered the name first. For example two similar names i.e. www.google.com and www.google.com.

iii. Cyber Destruction**:** Destruction /Vandalism mean destructing property of another. Or cyber destruction means destroying or damaging the data or information stored in computer when a network service is stopped or disrupted.

iv. Hacking Computer System**:** Finding out the weaknesses in networks and try to gain access to system/network by an illegal way is hacking. Changing in an unauthorized or illegal way. This requires little technical expertise and is common form of theft by employees altering the data before entry or entering false data, or by entering unauthorized instructions or using unauthorized processes; Changing, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions.

3) Cybercrime against organization

i. Hacking**:** It means unauthorized control/access over computer system .The act of hacking completely destroys the whole data as well as computer programs.

ii. Password sniffing: The programs that monitor and record the name and password of network users as they login, at site is Password Sniffing.

Denial of service attacks: Is basically where a computer system becomes unavailable to it's authorize end user. This form of attack generally relates to computer networks where the computer of the victim is submerged with more requests than it can handle which in turn causing the pc to crash. E.g. Amazon, Yahoo. Other incident occurs November, 2010 whistle blower site wikileaks.org got a DDoS attack.

iii. Denial of service attacks are designed to consume resources so that other users are unable to use the resources and are therefore ―denied service. In a Computer network environment, the key resources are CPU, memory, and bandwidth.

iv. Virus attack: A computer program that, when executed/implemented , replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication be successful, the affected areas are then starts abnormal working.

v. E-mail bombing/mail bomb: Sending a large no of emails to the victim to crash victim‗s E-mail account or server crash is E-mail bombing.

vi) Logic bomb: They are basically a set of commands or instructions where that instructions can secretly be execute into a program where if a particular condition is true can be carried out the end result usually ends with harmful effects. This suggests that these programs are produced to do something only when a specific event (known as a trigger event) occurs. E.g. Chernobyl virus.

vii) Trojan horse: A program or programs masks themselves as valuable tools but accomplish damaging tasks to the computer is Trojan horse. Particularly these are email viruses that can duplicate themselves, steal information, or harm the computer system.

IV. PREVENTION METHODS FOR CYBER CRIME

1. Use strong passwords.

a. Use separate ID/password combinations for different accounts, and avoid writing them down.

b. Make the passwords more complicated by combining letters, numbers, and special characters. Change them on a regular basis.

c. Use strong passwords with upper case, lower case, number and special characters and minimum of 6 characters.

d. Don't use passwords that contain names, birthdays, phone numbers, etc.

e. Don't share passwords across multiple services i.e. same password for Gmail, Credit Cards, Work, Twitter, etc.

f. Don't use sequential passwords for different services i.e. ABC10, ABC11, ABC12, etc.

g. Don't store your passwords under your keyboard, in your drawer, in Outlook, Gmail, Phone, password wallet software, etc.

h. Best place to store passwords is in your brain; second best is written on a piece of paper and kept in your wallet.

i. Never tell your password to anyone, including people from support, customer service, helpdesk, etc.

2. Secure your computer:

i. Enable your firewall: Firewalls are the first line of cyber protection/defense, they block connections from doubtful traffic and keep out some types of viruses and hackers.

ii. Use anti-virus/malware software: Prevent viruses from infecting your computer by installing and regularly updating anti-virus software.

3. Block spyware attacks.

4. Set up the latest operating system updates: Keep your applications and operating system (e.g., Windows, Mac, Linux) update with the latest system updates. Turn on automatic updates to prevent possible attacks on older software.

5. Protect your data: Use encryption for your most sensitive files such as health records, tax returns, and financial records. Make regular backups of all of your important data.

6. Secure your wireless network: Wi-Fi (wireless) networks are vulnerable to intrusion if they are not properly secured.

7. Protect your e-identity: Be cautious when giving out personal information such as your name, address, phone number, or financial information on the Internet. Ensure that websites are secure, especially when making online purchases, or ensure that you've enabled privacy settings (e.g., when accessing/using social networking sites, such as Facebook, Twitter, YouTube, etc.). If the user posts something by means of internet then that data will remain forever.

8. Avoid being scammed: Never reply to emails that ask you to verify your information or confirm your user ID or password. Don't click on a link or file of unknown origin. Check the source of the message; when in doubt, verify the source.

V. CONCLUSION

Cyber crimes affects every internet user in different manners. Different type's cyber attacks are discussed in this paper. Criminals have also adapted the improvements and advancements of computer technology to carry forward their own unauthorized and illegal activities. Certain defensive actions should be taken by all of us while using the internet which will assist in challenging this major threat Cyber Crime. The safety and well-being of citizens should be safeguarded. Everyone deserves a right to live in a secure environment, no matter in real-life or on the Internet.

Cyber crimes are happening in a wider way because some choose to take their political/religious protests online:

- Global reach of the Internet
- Support is quickly gained
- Online protests are sure to get attention
- Protestors are less likely to get caught

However, cyber-crime more serious than real-life crime, for the only reason that millions of web users are regularly get affected at once (as compared to perhaps one bank or store in a real-life robbery). When online business activities are interrupted, its leads to great embarrassment for customers and companies.

REFERENCES

1. Cybercrime: Criminal Threats from Cyberspace by Susan W. Brenner
2. cyber Crime: Issues, threats And Management, 2Nd Vol. by Atul jain
3. Understanding Cyberterrorism By Redins, Larisa
4. Case Studies of Cybercrime and Their Impact on Marketing Activity and Shareholder Value By Smith, Katherine T.; Smith, L. Murphy; Smith, Jacob L
5. Risk Factors in Computer-Crime VictimizationBy Kyung-Shick Choi
6. http://www.computerweekly.com/news/450404344/Top-10-cyber-crime-stories-of-2016
7. http://www.faronics.com/news/blog/7-types-of-cyber-criminals/