A Survey of Cyber Crimes

S.MISHRA[1]

P.G. Dept. Of Computer Science and Application
Jyoti Vihar, Sambalpur University, Burla, Sambalpur,Odisha,India
suchismitamishra52@gmail.com

C.S.PANDA[2]

P.G. Dept. Of Computer Science and Application
Jyoti Vihar, Sambalpur University, Burla, Sambalpur,Odisha,India
dr.chandrasekharpanda@gmail.com

Abstract- Now a days Cyber Crime is the most significant challenges in India .Cyber Crimes are generally referred as criminal activities that use computers or networks. It can range from fraud to unsolicited emails (spam). It can include the distant theft of government or corporate secrets through criminal trespass into remote systems around the globe. Characteristics and nature of Cyber Crime is important in helping research communities find ways to effectively prevent them. The internet is the electronic information field for such crimes. Such crimes have no space or time limitations and, naturally, there are no moral or legal barriers to them. Now it is a crucial challenge to us because day by day cyber crime is gradually increases. This paper provides a survey of Cyber Crimes that have actually occurred. The threat from Cyber Crime is multi-dimensional, targeting citizens, businesses, and governments at a rapidly growing rate. Cyber Criminal tools pose a direct threat to security and play an increasingly important role in facilitating most forms of organized crime and terrorism. This paper introduces some approach to prevent the various Cyber Crimes. To avoid Cyber Crimes there are many ways like, know how to recognize phishing, know the pitfalls of public Wi-Fi, use credit cards rather than debit cards etc. are discussed.

Keywords: phishing, identity theft, child pornography, online gambling, hacking, spamming, phreaking, malware

I. INTRODUCTION

Now a day's cyber crime is one of the most significant challenges. Cyber crime occurs due to the advancement of computer and information technology. A crime committed or facilitated via the Internet is a cyber crime. Cyber crime is any criminal activity involving computers and networks. "Cybercrime" combines the term "crime" with the root "cyber" from the word "cybernetic", which means to lead or govern. The most important difference between a cyber crime and a physical crime is that a cyber crime always happens in digital or virtual world. In the physical world, crimes are unavoidable but can be minimized by all kinds of mechanisms, such as regulations, laws, legislations, police etc. Similarly cyber crimes are unavoidable and should be punished by regulations, laws. There are no sound laws to protect users from cyber crimes because of the relatively brief history of information technology and peoples limited understanding of such crimes. It is difficult to make technical laws due to cyber crimes existence in the digital world. Therefore it is difficult to capture criminals and punish them. It is also difficult to collect evidence. Cyber crime generally is described as criminal activities that use modern information technology such as computer technology, network technology etc. There are all kinds of cybercrimes including illegal access (such as hacking), illegal interception, data interference, systems interference, misuse of devices, forgery etc[1]. The term cyber crime refers to criminal behavior carried out through a computer or network. It is also applied to some traditional crimes committed with the help of computers or networks.

II. HISTORY OF CYBER CRIME

Computers and networks came in the 1990s, hacking was done to get more information about the systems. Hackers competed against one another to win the tag of the best hacker. As a result, many networks were affected from the military to commercial organizations. However, with malicious software becoming ubiquitous during the same period, hacking started making networks and systems slow. When hackers became more skillful, they started using their knowledge and expertise to gain benefit by exploiting and victimizing others.

III. CYBER CRIME IN MODERN SOCIETY

Today, criminals that indulge in cyber crimes are not driven by ego or expertise. Instead, they want to use their knowledge to gain benefits quickly. They are using their expertise to steal, deceive and exploit people as they find it easy to earn money without having to do an honest day's work. Cyber crimes have become a real threat today and are quite different from old-school crimes, such as robbing, mugging or stealing. Unlike these crimes, cyber crimes can be committed single handedly and does not require the physical presence of the criminals. The crimes can be committed from a remote location and the criminals need not worry about the law enforcement agencies in the country.

IV. CATEGORIES OF CYBER CRIME

Cyber crimes are broadly categorized into three categories, named as crime against

(a)Individual
(b) Property
(c) Government

(a) Individual: This type of cyber crime can be in the form of cyber stalking, distributing pornography, trafficking and "grooming". Now a days law enforcement agencies are taking this category of cyber crime very seriously and are joining forces internationally to reach and arrest the perpetrators.

(b) Property: In the real world a criminal can steal and rob, even in the cyber world. In this case, they can steal a person's bank details and siphon off money; misuse the credit card to make numerous purchases online; use malicious software to gain access to an organization's website or disrupt the systems of the organization. The malicious software can also damage software and hardware.

(c) Government: Crimes against a government are also known as cyber terrorism. This category can cause panic amongst the civilian population. In this category, criminals hack government websites, military websites or circulate propaganda. The perpetrators can be terrorist outfits or unfriendly governments of other nations.

V. TYPES OF CYBER CRIME

Cyber crimes are spread due to the contribution of advance of computers and networks. According to the main roles of computers or networks, cyber crimes are categorized into following five classes.

A. computer or network is used as a tool in a criminal activity:

These are the cyber crimes in which computers or networks are used as tools, including spamming and criminal copyright violations, especially those facilitated through peer-to-peer networks [2].

B. The computer or network is the target of a criminal activity:

These are the cyber crimes in which computers or networks are the targets of criminal activities including unauthorized access (i.e. defeating access controls), malicious code, viruses, denial-of-service (DoS) attacks, and hacking attacks [3].

C. The computer or network is the place of a criminal activity:

These are the cyber crimes in which computers or networks are mainly the places of criminal activities, including theft of services (in particular, telecommunication frauds) and certain financial frauds [3].

D. Traditional crimes facilitated through the computers or the networks:

This category of crimes includes gullibility or social engineering frauds such as phishing, identity theft, child pornography, online gambling, securities fraud etc [2].

E. Other information crimes:

This category of crimes includes trade secret theft and industrial or economic espionage [3].

In the following, each category of cyber crimes has been elaborated in detail:

A. As A Tool

In this category copyright and spamming are discussed.

(a) Copyright: Copyright is a legal concept. It is enacted by government. The copy right gives the creator of an original work. The creator of an original work has the exclusive right to it for a limited time. It has the right to copy or to decide who can use the copy. Now days copyrighted materials are downloaded unlawfully and shared. The people are also selling the copyrighted materials such as VCDs, CDs, and DVDs [4].

(b) Spamming: Spam is an electronic junk mail or junk news group posting which are defined as any unsolicited email. Spamming usually refers to the abuse of electronic messaging and the indiscriminate sending of unsolicited bulk messages. Spamming is widely recognized as email spam .It has been similarly abused in other approaches such as instant messaging, the Usenet news group, web search engines, blogs, wikis, mobile phone messaging etc. Spam can be used to spread all kinds of viruses and malicious software for identity theft, distributing some malwares or worse.

B. As A Target

In this category Denial of Service, Malware, and Hacker are discussed.

(a) Denial Of Service: A DoS attack or Distributed DoS (DDoS) attack is a crime that renders computers or network resources inaccessible to their intended users or customers. Criminals are always interested in sites or hosts related to high profile servers, such as banks, credit card payment gateways and even domain name system (DNS) root servers [5].

The symptoms of DoS attacks are:

*unusually slow performance of network services

*unavailability of a particular website or even any website and

*an increasing number of spam emails.

(b) Malwares: Malware refers to designed to penetrate or destroy a computer system without the knowledge of the owner. The word malware combines the words malicious and software .The term “malware” is seldom used by computer users and many people are confused by the terms “malware” and “virus”. The term “virus” is inappropriately used in parlance to describe all kinds of malware, but not all kinds of malware are actually viruses. Malware refers to viruses, Trojans worms and other software that gets onto your computer without you being aware of them [6].

(c) Hacker: Hacking is a form of computer crime where one breaks into a computer system to achieve an unauthorized access to data or information. A hacker is someone who tries to explore systems or obtain unauthorized access to others computers through specific skills or knowledge. There are three kinds of hackers:

1-black hat hackers-People that always refers to with the term hacker is a black hat hacker.

2-white hat hackers-White hat hackers are ethical hackers.

3-gray hat hackers-Gray hat hackers are ambiguous in ethics.

C. As A Place

In this category phreaking is discussed.

(a) Phreaking: Phreaking is a slang term and it is used to describe criminal activities related to phones. The word”phreak” is a combination of the words “phone” and “freaks”. Such criminal activities are always related to those people working with or studying telecommunication systems, especially those familiar with public telephone networks and related equipments and systems [7].

D. Traditional Non-Cybercrimes

In this category phishing, Identity theft, child pornography, online gambling, cyber stalking, cyber terrorism are discussed.

(a) Phishing: It is the act of attempting to acquire sensitive information like usernames, passwords and credit card details by a trustworthy source. Phishing is carried out through emails or by luring the users to enter personal information through fake websites. Phishing refers to attempts to criminally and fraudulently gain sensitive information such as usernames, passwords, and credit card details by means of some public entities that run on electronic systems, such as online banks .Phishing uses email or instant messaging and directs users to enter their detailed information on the website. Phishers also target social networks through which they can gain a customer’s personal information for identity theft [8].

(b) Identity Theft: Identity is a severe fraud that may involve stealing money and obtaining other gains using others identity. Identity theft is a term used to describe fraud in which the criminal pretends to be someone else to steal money or get other benefits. It is also a crime for criminals to pretend to be someone else even if they do not steal an identity [9].

(c) Child Pornography: Child Pornography is the term used to describe the sexual abuse of children by means of pornographic material [10].With the help of the Internet; it is quite easy to spread images and video. Child pornography is illegal all over the world. Related production of such material is also prohibited .The main reason that such criminal activities continue is the profit that can be generated from the sale of such images. Photographs and movies are still being produced and purchased.

(d) Online Gambling: Generally it refers to gambling over the Internet. Gamblers (playing in places like online casinos) may be targeted by criminals who try to steal money from them by infecting their computers. It is certainly the case that Internet users who have financial transaction data are attractive targets for criminals. In these cases, criminals may use a 'raketracker' tool that allows users to monitor the house's take on their games. Using the tool, the criminal can access login details for a variety of well know online casinos. The criminals can then make money by setting up games between themselves and the compromised online gamblers.

(e) Cyber Stalking: Cyber stalking is stalking someone through the Internet or through other electronic means. It refers to an individual or group of individuals harassing another individual, group of individuals or organization through the internet or other communication technologies [11].Stalking is a criminal activity that consists of a series of continuous behaviors and each of them may even be entirely legal in themselves.

The main factors of cyber stalking can be identified as follows:

(a) False accusations: Many cyber stalkers aim to ruin the reputation of their victims. In order to disgrace their victims, the cyber stalkers may apply all different kinds of media such as news papers, Bulletin Board System (BBS), websites, blogs etc to spread false information about the victims [12].

(b) Attempts to gather information about the victim: The cyber stalker may try to approach the family or friends of the victim for detailed information about the victims [13].

(c) Turning others against the victim: Sometimes the cyber stalkers try to turn a third party against their victims for harassment purposes. They post the contact information of the victims, such as their names, phone numbers, addresses etc.

(d) Attacks on data and equipment: The cyber stalkers may send viruses in an attempt to damage the victims computer .The cyber stalkers use many methods to meet or target their victims such as search engines, online forums and blogs etc.

(f) Cyber Terrorism: Cyber terrorism can be defined as electronic attacks from cyber space from both the internal and external networks, particularly from the internet that arise from various terrorist sources with different set of motivation and are directed at a particular target.

E. Information Crimes

In this category Trade secret is discussed.

(a) Trade Secret: A trade secret is an advantage to the business. It should not be disclosed to public or competitors. Advantages are in different forms such as formulas, practices, processes, designs, instruments, patterns or compilations of information. To keep the trade secret the company will obtain the oaths of its employee not to disclose the companies’ technology and trade secret [14].

VI. HOW TO AVOID CYBER CRIMES

Prevention is better than cure. So to avoid cyber crimes following points are discussed:

(1) At the time of opening a bank account we have submitted all our related information to them. Subsequently the bank will not ask us to supply this information. If any message regarding supply of any message regarding supply of account number, password, PIN etc is received it will lead a phishing attempt.

(2) Now smart phones are same as a computer or laptop. So step should be taken to protect the smart phone like our laptop or computer. To protect smart phones we have to create strong password and update the operating system frequently.

(3) In Face book and other social media do not give your personal information. Here other security questions like “first school you attend”, “name of favorite pet” etc. may be given.

(4) Many websites like creditcards.com suggests that to avoid public wireless internet connections.

(5) In public computers like hotel, malls do not access your accounts or personal information because they have software to records your passwords and account numbers.

(6) Credit cards are more secure than debit cards at the timing of online shopping.

(7) You should have to check your credit reports regularly to avoid cyber crime.

(8) There are many suspicious E-mails in mail-id. So do not click on links in suspicious emails.

CONCLUSION

Due to the great advancement in computer technology, there exist different kinds of cyber crimes. Anyone could be attacked by a cyber criminal. Everyday serious cyber attacks happen and we should have the basic preparation to protect ourselves. Self awareness is the best way to avoid cyber crime. Everyone can also install firewalls to protect themselves from many attacks and can avoid installing unknown software. In this paper, we categorized cybercrimes in to several different classes and explained each category. The main purpose of the paper is to help people realize the threats and attacks and to learn from these attacks to protect themselves.

REFERENCES

[1] Moore R.Cybercrime: Investigating High-Technology Computer Crime. Anderson Publishing: Cleveland, Mississippi, 2008.

[2] Bantekas I, Nash S. International Criminal law 2/E, Routledge Cavendish: London, 2003.ISBN 1859417760[retrieved on 20 June 2008].

[3] CyberForensics2008.Availablefrom: http://www.santoshraut.com/forensic/cybercrime.html[accessed on 25 April 2010].

[4] Copyright. Available from: http://en.wikipedia.org/wiki/copyright [accessed on 25 April 2010].

[5] Yuval F, Uri K, Yuval E , Shlomi D, and Chanan G. Google Android: A comprehensive Security Assessment. In the proceeding of IEEE security and privacy, Los Alamitos, CA, USA: IEEE Computer Society 2010; 8(2):35-44.

[6] Available from: http://en.wikipedia.org/wiki/malware[retrieved on 20 June 2008].

[7] Schenker L.Pushbutton calling with a Two-Group Voice-Frequency code, The Bell System technical journal 1960;39(1):235-255.Available from : http://www.alcatel-lucent.com/bstj/vol 39-1960/articles/bstj 39-1-235 pdf.

[8] Identity theft .Available from :http://en.wikipedia.org/wiki/Identity-theft[retrieved on 25 April 2010].

[9] Leyden J. Trojans Fuel ID theft boom. January 2007.Available from: http://www.theregister.co.uk/2007/01/18 mcafee-id-theft-trends/ [accessed 25 April 2010].

[10] Wolak J, Finkehor D, Mitchell K, Ybarra M. Online “predators” and Their Victims. American Psychologist February 2008; 63(2):111-128.

[11] Royakkers L. The Dutch Approach to stalking Laws. California Criminal Law October 2000 Vol 3 .Available from: http://boalt.org/CCLR/V3/V3royakkers.PDF .

[12] Cyberstalking.Availablefrom: http://www.ncvc.org/ncvc/main.aspx?dbName=Documentviewer and Document ID=32458 [accessed 25 April 2010].

[13] Moravekj D. SocialNetworks- The Change ofCommunication Paradigm 2008.Available from: http://noebius.com/pdf/moravek-social-networks-part1.pdf .

[14] Trade secret. Available from: http://www.absolute astronomy.com/topics/Trade-secret [accessed 25 April 2010].