IJSTE - International Journal of Science Technology & Engineering | Volume 5 | Issue 8 | February 2019
ISSN (online): 2349-784X

A Review Paper on Cyber Crime

Mohammad Faiz khan
Student
Department of Information & Technology
Chandigarh University, Gharuan, Punjab, India

Sanjam Singh
Student
Department of Information & Technology
Chandigarh University, Gharuan, Punjab, India

Er. Preeti Rani
Assistant Professor
Department of Electrical Engineering
Chandigarh University, Gharuan, Punjab, India

Abstract

Cybercrime is one of major problem that people face now a days and it effects the individual, organizations and even the Government. Cybercrime is basically a crime in which an offence is committed against an individual or group of people and itharms their emails, websites and mobile phones. This paper introduces review on cybercrime in detail.

Keywords: Financial Crimes, Cyber Stalking, Telecommunication Frauds, E-Mail Related Crimes, Cyber Criminals, Email Spoofing, Email Bombing

I. INTRODUCTION

The term crime is denoted as an unlawful act which is punishable by a state. Crime is also called as an offense or a criminal offense. According to the authors in, cyber is a prefix used to describe a person, thing or idea as a part of the computer and information age. It involves computer or computer networks. A computer network is basically the collection of communicating nodes that helps in transferring data across. The nodes at any given time could be a computer, the laptop, smart phones etc. Cybercrime encompasses any criminal act dealing with computers and networks. It includes crime conducted through the Internet. The Internet is basically the network of networks used across for communication and sharing of data. Cybercrime also known as the computer crime is the use of an instrument for illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. With the advancement of the Internet technologies like the 2G and 3G, the global village is effectively sharing and communicating vital data(s) across the network.

Fig. 1: cybercrime

II. CYBER CRIME

Cybercrime encompasses a wide range of crimes including stealing people's identity, fraud and financial crimes pornography, selling contraband items, downloading illegal files etc. Some of the popular and alarming crimes in the cyber world are discussed below:

A. Financial Crimes

The criminals of credit card fraud get information from their victims often by impersonating a Government official or people from financial organizations asking for their credit information. The victims fall prey to this without proper inquiries and give away their credit card information to these criminals.

B. Cyber Pornography

Pornographic websites which allow downloading of pornographic movies, videos and pictures, on-line pornography magazines (photos, writings etc.), all come under this category. The study made by the UK Home Affairs Committee Report on Computer Pornography (House of Commons, 1994) says that "Computer pornography is a new horror" (House of Commons, 1994:5).

C. Drug Trafficking

Drug traffickers contribute a major part of cybercrime to sell narcotics using the latest technologies for encrypting mails. Since there is no personal communication between the buyer and dealer, these exchanges are more comfortable for intimidated people to buy illegal drugs and even other items.

D. Cyber Terrorism

Cyber terrorism may include a simple broadcast of information on the Internet about bomb attacks which may happen at a particular time in the future.Cyber terrorists are people who threaten and coerce an individual, an organization or even a government by attacking them through computers and networks for their personal, political or social benefits.

E. Online Gambling

On-line gambling offered by thousands of websites that have their servers hosted abroad.

III. TYPES OF CYBER CRIME

There are different types of cybercrime today. But the eight most common ones are:

A. Theft in the Services of Telecommunication

Individuals and criminal organizations can gain access to the switchboards of an organization's switchboard and obtain the access to their dial-in or dial-out circuits. The criminal is usually asked to pay a fine with a short amount of jail time.

B. Piracy of Telecommunication

When the creators of a particular work are not able to gain profit from their own creations, it leads to severe financial loss and a great effect on creative efforts generally.

C. Laundering E-money and Evasion of Taxes

Central bank supervision will be bypassed by the development of the informal banking institutions or the parallel banking systems. There is no separate law for this type of crime committed using computer and a network, but it falls directly under the laws which cover these offenses in general.

D. Illegal Interception of Telecoms Signals

The great and fast development in telecommunications allows new opportunities for electronic eavesdropping. The existing laws today, does not prevent one from monitoring a computer radiation from a distance.

E. Fraud in Transfer of Electronic Funds

Electronic transfer systems are proliferating, and the same goes with the risks that such type of transactions may be intercepted or diverted. With the usage of electronic fund transfer system, there is no doubt that this system will enhance the risk. Year 2009 showed a hike of about 559.7 million U.S. dollars and later by 2017 the monetary damage grew to 781.84 million U.S. dollar which is certainly alarming.

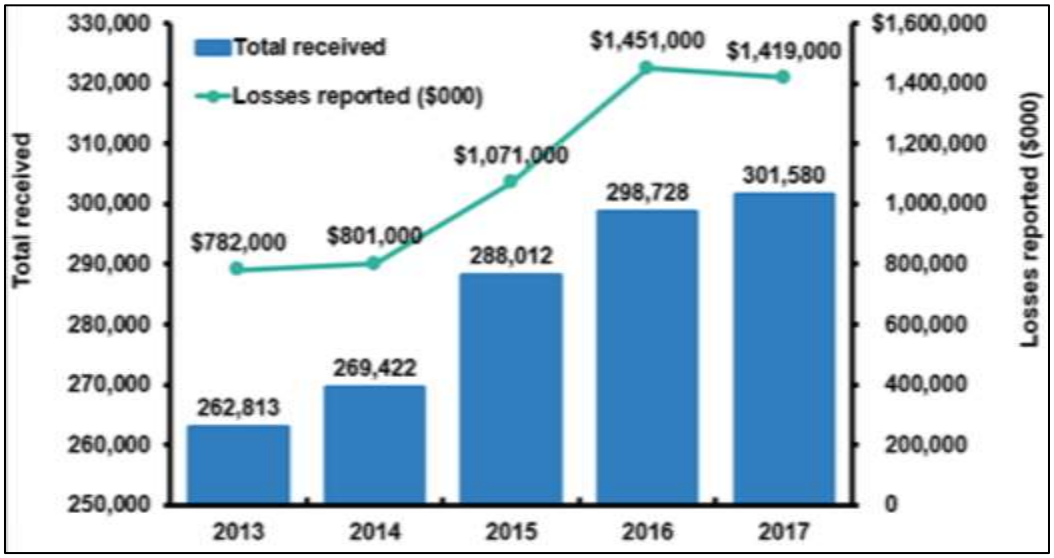


Fig. 2: Amount of monetary damage caused by cybercrime from 2013 to 2018(in million U.S. dollars) reported to the IC3.

Symantec – A famous Security Firm, carried out a detailed study and has been able to find out the top ranked 20 countries that were facing and/or causing most of the activities of cybercrime. The design was made to trick users so that the computer user discloses their personal information or banking account information.

In its further investigation, Symantec was successfully able to acquire the data including the number of bot-infected systems. These systems were meticulously controlled by the cybercriminals.

The higher rate of cybercrime was found to be in the United States of America. This could be because the country is well facilitated with the broadband connection providing uninterrupted internet connection.

Table 1 shows the countries that had been the victims of cybercrimes such as sharing malicious computer activities, spam messages, phishing etc. The table 1 shows, the six factors;

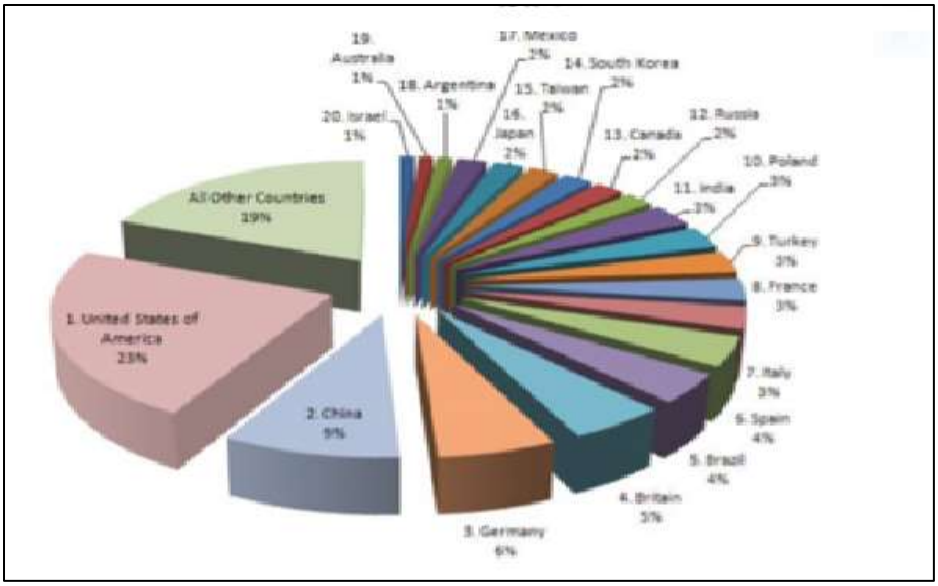
1) Share of malicious computer activity,
2) Malicious code rank,
3) Spam zombies rank,
4) Phishing web site hosts rank,
5) Bot rank and
6) Attack origin,

These factors contribute to authenticate its cybercrime ranking as conducted by Symantec security organization.

Table – 1
Country lists with six contributing factors to cybercrime

Country	Share of Malicious Computer Activity	Malicious Code rank	Spam Zombies rank	Phishing website hosts rank	Bot rank	Attack origin rank
USA	23%	1	3	1	2	1
China	9%	2	4	6	1	2
Germany	6%	12	2	2	4	4
Britain	5%	4	10	5	9	3
Brazil	4%	16	1	16	5	9
Spam	4%	10	8	13	3	6
Italy	3%	11	6	14	6	8
France	3%	8	14	9	10	5
Turkey	3%	15	5	24	8	12
Poland	3%	23	9	8	7	17
India	3%	3	11	22	20	19
Russia	2%	18	7	7	17	14
Canada	2%	5	40	3	14	10
South Korea	2%	21	19	4	15	7
Taiwan	2%	11	21	12	11	15
Japan	2%	7	29	11	22	11
Mexico	2%	6	18	31	21	16
Argentina	1%	44	12	20	12	18
Australia	1%	14	37	17	27	13
Israel	1%	40	16	15	16	22

From the pie chart given at Fig. 2, it is quite evident that United States of America had suffered a lot due to cybercrime. The loss that had incurred has been tremendous other countries as well. China stands at the second position. Then the countries like Germany and Britain stood next, who had to bear the loss, occurred due to cybercrime. Countries like Brazil, Spain share almost the same percentage of cybercrime happening. Similarly, Italy, France, Turkey and Poland stands with the same percentage of cybercrime caused at their countries respectively. India share 3% of the malicious computer activities. Argentina, Australia and Israel share only 1% of the malicious computer activities. Mexico has the highest rank for hosting the phishing websites. Australia ranks the highest for bot- activities.



Pie Chart 1: cybercrime in top 20 countries

IV. CRIME ON THE INTERNET

Crimes committed on the Internet by using the Internet and by means of the same, are mainly called Internet crimes. According to David Wall, the term Cybercrime symbolizes to the occurrence of the harmful activities done with the digital devices mainly over the Internet. The Cybercrime practically doesn't refer to the law and it is the concept that is created by the media to a greater extend. In general term computer crime is a crime that encompasses crimes such as phishing, bank robbery, credit card frauds, child pornography, kidnapping of children by means of chat rooms, creation or the distribution of viruses and so on. All these are facilitated crimes related to computers. Some crimes which are committed on the Internet are exposed to the world and some are hidden until they perpetrated against someone or company.

A. E-mail Related Crimes

Electronic mail has rapidly become the world's most preferred means of communication. Across the globe, millions of e-mail messages are sent and received every day. E-mail, like any other means of communication, is also being misused by criminals. It has become a powerful tool for criminals due to the ease, the speed of transfer and its relative anonymity.

1) E-mail Spoofing:

It is found in that an e-mail that appears to originate from one source while it is actually being sent from another source is called e-mail spoofing. Email spoofing is usually committed by falsifying the e-mail address of the sender and/or the name. to send an e-mail, one usually has to enter the following information

1) The e-mail address of the receiver.
2) The e-mail addresses of the receivers (referred to as C for carbon copy).
3) The e-mail addresses of the persons who will receive a copy (referred as CC for carbon copy).
4) A subject for the message, which is a short title or a short description of the message.

2) E-mail Defamation:

Cyber defamation or cyber slander often proves to be very dangerous and even fatal for anyone with even a little knowledge of computers to become blackmailers often by threatening their victims through e-mails.

3) E-mail Frauds:

Financial crimes are commonly committed through e-mail spoofing. It is becoming easier to assume an identity as well as to hide one's own identity. The criminal knows very well that there is minimum chance of his being identified.

V. WHO ARE CYBER CRIMINALS?

Cyber criminals range from a wide variety of age groups:

A. Kids(age group 9-16)

Although it is hard to believe, kids can also be cyber criminals knowingly or unknowingly. The most amateur hackers comprises of teenagers. To these teenagers, it appears to be a matter of pride to be able to hack into a computer system or to a website. They may also commit the crimes without actually knowing that what they are doing is a crime.

B. Organized Hacktivists

Hackers who come together with a particular motive are called hacktivists. These groups mostly operate on a political basis. While in other cases, their motives may be social activism or religious activism or any other.

C. Professional Hackers

Extensive computerization has led to the storage of information in electronic form in business organizations. Hackers are employed by rival organizations to steal other industrial information and secrets which can prove to be beneficial for them. If hacking can retrieve the required information from rival companies, the fact that physical presence required to gain access is considered unnecessary. This also leads to the temptation of companies hiring professional hackers to do their dirty jobs.

VI. CONCLUSION

From this study made, it has been found that there are many ways and means through which an individual can commit crimes on cyber space. Cybercrimes are an offense and are punishable by law. In section 2, we have seen a brief discussion of the enlarging areas of cybercrimes.

In section 3, we have seen the common types and areas where cybercrime occurs very frequently. We have also discussed the consequences of cybercrime that are causing tremendous financial losses in many countries, especially in the areas of sales and investments. Different fines and penalties have been laid down for this category of crime.
Section 4 discusses about the different crimes on the net that are related to electronic mails.

These crimes involve spoofing of mail, e-mail bombing and spreading malicious codes via emails. Furthermore, we have seen the different cyber criminals, ranging from the most amateur teenage hackers to the professional hackers that are often hired by rival organizations for hacking the into other company's system.

It is therefore very important for every individual to be aware of these crimes and remain alert to avoid any loss. To ensure justice to the victims and punish the criminals, the judiciary has come up with some laws known as Cyber Laws. Hence, it is advisable to each and every individual to know these laws. Besides, the cybercrime cannot be simply called as a Technological problem. Instead, it is an Approach based problem because it is not the computers that are harming and attacking the organizations instead it is the humans who are exploiting the technology to cause the damage. Therefore, it is we who need to be alert to figure out the different approaches that such criminals can take. There is a need to have intellectual mindset to sense such situation that may lead to such damages. The solution to such crimes cannot be simply based on the technology. The technologies can just be one such weapon to track and put a break to such activities to some extent.

REFERENCES

[1] Admiral Dennis C. Blair, Annual Threat Assessment, House Permanent Select Committee on Intelligence, 111th Congress, 1st sess., 2009.
[2] Audry Watters, Read Write Cloud, RWW Solution Series, 2010
[3] Ajith Abraham1, Crina Grosan2, Yuehui Chen3, Cyber Security and the Evolution of Intrusion Detection Systems, School of Computer Science and Engineering, Chung-Ang University, Korea 2Department of Computer Science Babes-Bolyai University, ClujNapoca, 3400, Romania 3School of Information Science and Engineering Jinan University, Jinan 250022, P.R.China
[4] Cisco, Cisco 2009 Annual Security Report: Highlighting Global Security Threats and Trends, December 4, 2009.
[5] AmichaiShulan, Application DefenceCenter (ADC), AmichaRegu-larlyLectures, Security, 2011
[6] Booz Allen and Hamilton, Reports, ―Top Ten Cyber Security Trends for Financial Services‖, 2012