International Journal of Latest Trends in Engineering and Technology
Vol.(10)Issue(3), pp.186-189
DOI: http://dx.doi.org/10.21172/1.103.32
e-ISSN:2278-621X

CYBERCRIMES OVER INTERNET AND COMPUTER NETWORKS: RISING THREATS AND THEIR FORENSIC SOLUTIONS

Anuradha[1], Ashish Kumar Sharma[2]

Abstract- As there are exponential changes in technology and its use is increased in different organizations, the methods of cybercrime and digital forensics are also being enhanced to face it. Cybercrime is an emerging threats posed by this incredible rise in digitization. Cybercrime means any crime that involves a computer or any electronic devices which process the digital data and use either as a target or as a weapon. Cybercrimes thereby take place in many forms like illegal access and theft of data, intrusion into devices and fraud which is a big concern amongst all the users. To control and investigate cybercrime, the investigators use various Digital forensics methods and mechanisms. Digital forensics is the procedure of investigating computer crimes in cyber world. Many researchers have been done a lot in this area to help forensic investigators to resolve the existing challenges with different methodologies designed by them. Still the desired technologies and tools are not that much efficient that they can control the occurrence of different types of cybercrime activities. This paper explores the need to identify and remain safe from the effects of cybercrime keeping in mind that the recent activities taken place in the world and offering various solutions to protect ourselves from it. In this paper few case studies have also discussed while innovative suggestions for future cyber security proposed.
Keywords – Hacking, Information Security, Cyber threats, Phishing, Cyber Safety, Digital Data, Digital Forensics, Internet, Cybercrime.

1. INTRODUCTION OF CYBER CRIME

Cybercrime is a criminal activity which is committed on the internet and on the computer network or devices. It is a type of crime against an organization or an individual in which computer is used as a target or as a weapon. These are the specific offences that are being committed against the individuals or the groups of individuals with a clear criminal motive to intentionally cause harm to the reputation of the victim or to cause the physical or mental harm to the victim directly or indirectly with the help of the modern telecommunication network available such as the internet (chat, emails, notice boards, viruses) and mobile phones (SMS, MMS, Calls). For example to understand the cybercrime let us see its basic types:

Data Piracy: It means reproduction of digital data and its easy distribution of print, graphics, sound and multimedia combinations even there may be a use of copyrighted materials for personal use. [1]

Pornography/Child pornography: It is the unethical and illegal distribution of sexually implicit material especially involving children.

There are other situations of Computer Oriented Cyber Crime too where Computer is the target of crime like:

Computer Hacking: Theft of Information from computer storage devices (hard disk, USBs) like stealing username, password and altering these information is called hacking.

Internet Forgery: It means the duplication or the reproduction of documents, certificates, copy right protected materials and fake currency.

[1] Research Scholar, Department of CFIS, Ganga Institute of Technology & Management, Kablana, Jhajjar, MDU-Rohtak, Haryana, India
[2] Assistant Professor, Department of CFIS, Ganga Institute of Technology & Management, Kablana, Jhajjar, MDU-Rohtak, Haryana, India

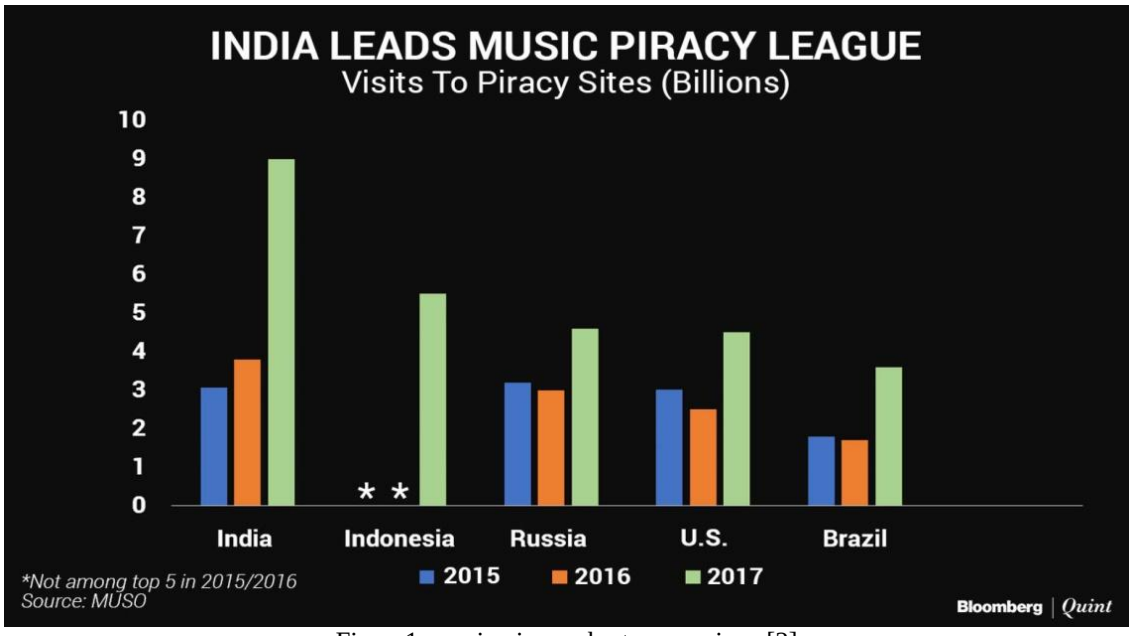

Figure1: music piracy chart comparison [2]

Cyber terrorism: It means E-murder or homicide or suicide or Spyware. [2]
There are two main types that define cybercrime:
1) Target computer network or devices such as viruses, malware, or denial of service attacks.
2) Crime that are facilitated by computer network or device like cyber-stalking, fraud, identity theft, phishing, extortion etc.

In these days cybercrime is not limited to the boundaries of countries and now be considered as a global epidemic. It covers such a broad scope of criminal enterprise that "The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard then with a bomb".

2. CAUSES OF CYBER CRIMES

They are easy to access: The main problem faced in securing a computer system from unauthorized access is that there is every possibility of violation of technologies by stealing the access codes, recorders, pins, retina imagers etc. that can be used to fool biometric systems and bypass firewalls to get past many a security system. [3]
Negligence: There are possibilities of not paying attention in protecting the system. This negligence gives the criminals control to damage the computer.
To get Revenge or other Motivation: There may be some motivation from greed to master the complex computer systems with a strong will to cause loss to the cybercrime victim. This majorly involves youngsters or those who have a lust to make quick money and so they tamper with data like e-commerce, e-banking or fraudulent transactions. [4]

3. INTRODUCTION OF DIGITAL FORENSICS

Today Digital Forensics activities are very important tool for solving crimes committed with computers, as well as for solving crimes against people where evidence may reside on a computer. The science of Digital Forensics includes identifications, extractions, analyzing and presentation of the digital evidences that has been stored in the digital devices. Evidence obtained in a computer forensic investigation can be useful in criminal, civil, or corporate investigations, but different legal rules may apply.

4. TOOLS AND TECHNOLOGIES CONSTRAINTS IN INDIA

For better cyber forensics research and investigation purpose, developers have created various computer forensics tools. Police departments and investigation agencies than select these tools based on various factors including their budget and available expertise in the team.

- Digital Forensics Framework
- Open Computer Forensics Architectures
- Computer Aided Investigative Environment (CAINE)
- Mobile edit Forensics
- SIM tools
- BitPim
- ATHENA

5. CYBER CRIME AND DIGITAL FORENSICS ON MULTIPLE PLATFORMS

There are multiple platforms where cybercrime and Digital forensics are used. Mobile Device Forensics Originated in Europe and focused on the GSM SIM card. In mobiles there are many operating systems where cyber security is used and these are Android, Windows, Blackberry, IOS apple, Intel, BADA, Palm OS, Open web OS, Maemo, Verdict etc. Mobile Operating System is different from Computer System Operating System. In computer system there is also some Operating System like Windows, MS-DOS, Linux, Unix, Unicox, IBM etc. [5]

1) Android Operating System: Android is the open source and „free to use" operating system for mobile devices developed by Google. However, this open-development feature also poses challenges to securing sensitive user data and protecting users from malicious attacks, such as phishing applications.

2) Blackberry OS: Blackberry operating system which was not explored by anyone because of security person. Blackberry was not safe so it will be banned.

3) Windows OS: Most of the cybercrimes are happen on windows operating system. New forensic challenges arise with the introduction of newly released and latest windows operating systems.

4) Linux OS: The Internet is made up of a majority of Linux systems. Learning the basic Linux concepts will help the Investigator effectively interview witnesses and suspects?

6. CYBER CRIME INVESTIGATIONS

Here are some of the case studies to elaborate on the cyber threats and various methods of defending against than these cyber-attacks:

Case 1: Phishing Case Study

A Doctor from Gujarat province had registered a cybercrime and state that some people ("perpetrators") have perpetrated illegal acts through misleading fake emails ostensibly emanating from ICICI Bank's email ID. These acts have been perpetrated with the solid intentions to defraud the bank's Customers. When the investigation were carried out with the help of the all e-mails received from the customer, their bank account IP details & domain IP information, than the place of offence at was searched for evidences.

Case 2: On line credit card Cheating and Forgery Scam

Another one of the most famous cases of 2003, A case has been registered against Amit Tiwari, who was a 21yr old engineering student and had so many names, bank accounts and clients with an ingenious master plan to defraud a Mumbai based credit card payment processing company, CC Avenue of nearly Rs. 900, 000.

7. DEFENDING AGAINST CYBER CRIMES

Securing and monitoring of wireless and network access points along with network-attached devices by securing interfaces of public networks.

To prevent insider attacks on agency networks access rights to files should be controlled and access should be granted only on as required for the performance of job duties. [6]

To prevent against exploitation:

A periodic scanning of the computer systems is must for malware with anti-spyware programs.

Denial of all inbound traffic by default through the perimeter defense.

There must be a provision for the training on an annual basis on cybercrime awareness that, in part, cautions against downloading software programs from the Internet without appropriate agency approval.[7]

8. CONCLUSIONS

The growth of cybercrime is exponentially very high all over the world and the proper and adequate education is needed to reduce the risk associated with various types of cybercrimes. Present study shows that with the increasing rate of cybercrimes more detection techniques along with educating the internet users about how to be safe online is needed to be established along with complete guidance to know about the pros and cons of the web world even before entering it. Understanding the behavior of the cyber criminals and impact of cybercrimes on society will definitely help to find out the sufficient means to overcome the situation.

As we can easily see that more and more tools are being developed and are made available to the cyber forensics investigators to facilitate them so that they can easily acquire the digital evidences and solve the related problem in more

efficient and effective manner. This exponential development of computing devices requires new and latest methods and tools to be used by the cyber forensic investigators in order to find the evidences that can be presented in the court of law. Here we have also discussed the various platforms that are much more secure for the users so that they can't be an easy target of the different cyber criminals over the internet.

9. REFERENCES

[1] Kshetri, Nir (2005) "Pattern of global cyber war and crime: A conceptual framework, " Journal of International Management, Elsevier, vol. 11(4), pages 541-562

[2] https://www.bloombergquint.com/business/2018/04/12/mukesh-ambanis-cheap-data-fuels-indias-piracy-addiction#gs.r9tmRAY by Nishant Sharma, MUSO

[3] Kshetri, Nir (2005) "Information and communications technologies, strategic asymmetry and national security, " Journal of International Management, Elsevier, vol. 11(4), pages 563-580, December.

[4] Michael Massourakis & Farahmand Rezvani & Tadashi Yamada (1984) "Occupation, Race, Unemployment and Crime In a Dynamic System, " NBER Working Papers 1256, National Bureau of Economic Research, Inc.

[5] Panu Poutvaara & Mikael Priks (2005) "Violent Groups and Police Tactics: Should Tear Gas Make Crime Preventers Cry?, " CESifo Working Paper Series 1639, CESifo Group Munich.

[6] Investigation of Different Constraints in Cybercrime & Digital Forensics by Shallu Kotwal, Dr. Jatinder Manhas.

[7] Ying-Chieh Chen, Patrick S. Chen, Jing-Jang Hwang, Larry Korba, Ronggong Song, George Yee, (2005) "An analysis of online gaming crime characteristics", Internet Research, Vol. 15 Iss: 3, pp.246 - 261

[8] Inside of Cyber Crimes and Information Security: Threats and Solutions 1Sunakshi Maghu*, 2Siddharth Sehra and 3Avdesh Bhardawaj.