Xournals

Academic Journal of Forensic Sciences

ISSN: 2581-4273 | Volume 02 | Issue 01 | April-2019

Cyber Crimes Becoming Threat to Cyber Security

Mirdul Sharma[1], Satvinder Kaur[2], Ranjeet Kumar Singh[2]

Available online at: www.xournals.com

Received 20th January 2019 | Revised 16th February 2019 | Accepted 18th April 2019

Abstract:

Modern age is the age of technology, in today's world peoples are using many devices or gadgets to make life simple. Development in technology helps in connecting people to the world, but misuse of technology in cyber world cause cybercrimes. Although, cybercrime can have dangerous impact on world. Cybercrime is a crime include computers or gadgets in which a system (computer) can be a target of the crime, tool of the crime or hold evidence of the crime. Basically cybercrime defined as criminal activity which happen over the Internet, by the peoples for their personal benefits. Following examples such as malware, fraud, and virus scripts, remote access Trojan's, IOT etc. The only secured computer in the world that is powered off, the objective of my paper is not to put a damper on the flourishing growth of technology but rather to create awareness that we as individual can appreciate and learn to mitigate the risks. Earlier cybercrimes was committed only by small groups. Now it is discovered that there is very complicated cybercriminal networks alliance at global level to commit crimes. Peoples that take part in cybercrimes want to use their skills to gain profits. In the present study the paper reviewed on the basis of the major threat on the world implementing or affecting the individuals in their routine life involving both the professional and personal manner. They are using their skills to exploit people and data theft as cyber criminal's find it easy to earn money. Cybercrimes have become big threat to cyber security which means protecting data, networks, programs and other information from unauthorised or unattended access.

Keywords- *Cyber Crime, Cyber Security, Internet, Criminal, Malware, Trojan, Virus*

Authors:

1. Department of Electronics and Communication, Nirma University Ahmedabad Gujarat, INDIA.

2. Sherlock Institute of Forensic Science, Delhi, INDIA

Introduction

The human is causing more harm to the society by using the knowledge in the wrong way and taking the medium for the purpose of harming and doing crime. When we talk about the information and its protection, information restriction and information security turns into a big concern. Is our own information extremely safe on the internet? It is very difficult to ensure anyone that our data on internet or on our system is completely safe, the rapid growth of cyber-crimes and new techniques are introducing day by day, it became very difficult to come with an instant solution to every cyber-crime. The major objective of this review is to provide awareness towards cyber-crimes, cyber laws and threats towards cyber security. There are five major concerns of cyber security, organised cyber-crime, cyber-crime trading, ransomware, smishing, hacktivism. In the world of technology only your mobile phone knows all your secrets like bank accounts passwords, email passwords, contacts etc. and by adding third party apps in your computer or mobile phone and providing them permission to excess your system, everyone is getting prone for cyber-crimes

In coming time a big technology wave is going to hit shores of cyber world IOT (internet of things) look around you and imagine if every object you see is capable of identify, communicate, locate, sense, compute, very soon if not already your pen, watch, shoes and even clothes are going to connect with internet having IP addresses, it is stated that there will be 21 billion IOT devices by 2020 and they will communicate with each other. An entire nation can be crippled by a cyber-attack on its critical infrastructure like power grid shut down or water supply and many more other. (Li, Xu, 2017). Ransom malware, or ransomware, is a sort of malware that lock or encrypt client's files or individual documents and requests emancipate installment so as to recover get to the same as before. The soonest variations of ransomware were created in the late 1980s, and installment was to be sent by means of snail mail. Today, ransomware creators request that installment be sent through cryptographic money or charge card. (Liska, Gallo 2016). An appropriated disowning of administration (DDoS) assault is a malignant endeavour to disturb typical traffic of a focused on server, administration or system by overpowering the objective or its encompassing framework with a surge of Internet traffic. DDoS assaults accomplish adequacy by using different traded off PC frameworks as wellsprings of assault traffic. Abused machines can incorporate PCs and other organized assets, for example, IOT gadgets. From an abnormal state, a DDoS assault resembles a car influx obstructing with roadway, keeping standard traffic from touching base at its ideal goal. **(Bhattacharyya, Kalita 2016).**

Malware is basically a malicious software or any malicious program or code which is harmful for our systemUnfriendly, frightful, malware tries to attack, harm, computer frameworks, systems, tablets, and cell phones, regularly by assuming incomplete responsibility for a gadget's tasks. Like the human influenza, it meddles with typical working. Malware is tied in with making cash off you illegally. Despite the fact that malware can't harm the physical equipment of frameworks or system gear, it can take, encode, or erase your information, modify or control CPU functions, and keep an eye on your PC movement without your insight or authorization. **(Aycock 2016).**

There are three major categories' of cyber-crime, cyber-crime on individual, cyber-crime on propriety, cyber-crime government. Cyber-crime on individual includes cyber stalking, pornography or sharing anything malicious online. Cyber-crime on propriety includes stealing information or money from an organisation by using malicious codes. Cyber-crimes on government is most uncommon crime but most serious offence it includes hacking government websites, military websites these type of criminals are known as terrorist and these type of criminal activities are known as cyber terrorism.

The concept of cyber-crime depend upon underground economy, underground economy is basically an economy that considered illegal because their trading ways are unlawful in nature cyber-crime and underground economy are basically connected with each other

There are numerous complexity of cyber security discussed on the basis of both economic, social, cultural, political as well as military point of view. The different activities which are inclusive to the security audits, authentication process, access management and any more. It can be best defined basically by the analysis and examination of the strength and exposure of software and hardware utilize by the country's both monetary and political infrastructure. It also include the research and analysis which are basically for the purpose of protecting and implementing those vulnerable activities and quality **(Maskan et.al, 2013).**

Review of Literature

Reddy (2016), discussed about the various different categories of cyber-crime and its impact on the professional and business aspects. The paper follows the numerous preventive measure which is required for the purpose of controlling the widespread cyber-crime. In the present study, he focussed on the effect of crime which is not only controlled by applying different judicial laws but also the different ethics and morals so that it influence the preventive measure of the crime. He also distinguish two kinds of cyber-crime which involve TYPE I TYPE II, here TYPE I includes phishing attacks, data theft using Trojan horse, banking fraud and encrypted virus scripts TYPE II include cyber stalking, extortion stock market manipulation, complex corporate espionage, child predation and travel scams . According to him the four major categories of cyber-crime are cyber-crime against the person , cyber-crime against propriety ,cyber-crime against government ,cyber-crime against whole society the major control of the author is towards the prevention of cyber-crimes which include avoidance of disclosing any personal information to anyone, updated antivirus software for the purpose of protecting against nremurous virus attack, the involvement of controlling various steps for both national and international level and many more.

Kharb (2016), discussed about the developing threat of cyber-crimes and the current laws must be continually assessed and changed as needs to be confront the difficulties originating from the cyber world. In present study, he talked about the digital violations as one of the difficulties for cyber laws, the primary accentuation of the paper rotates around the difficulties looked by cyber laws in controlling cyber-crimes. According to him cyber violations in the cyber society can be fundamentally partitioned into 3 noteworthy classes' cyber-crime against person, cyber-crime against property, cyber-crime against government. He also talked about the advantages and drawbacks of the India's first cyber law IT Act in 2000 It gives the lawful foundation to E-commerce in India yet additionally in the meantime, offers forces to the police to enter and look, with no warrant, any open spot to nab cyber lawbreakers and avoiding cyber-crimes. Lastly, they also focussed on the future approach regarding the implementation of new laws or amendment in existing laws for making this approach more active and prominent.

Ramdinmawii, Singh and Sharma (2014) discussed about the effects of cyber-crimes on society, organization and government including some connection with the cyber laws and punishment for cyber criminals. In the present study, they focused about the basic zones where cybercrime generally happens, email related violations and a portion of the contextual analyses identified with cybercrimes. The major focus is on the crimes which is widespread because of the email medium. Here they cover all the probable aspects including the impact of cyber- crime on numerous aspects and also how the cyber threat create problems in day to day life of an individual. The major concern cover cyber pornography, cyber stalking drug trafficking and many more. They justified their work by discussing different case studies encountered in the same scenario. The very wisely said by the authors in the paper that the basic cause of attacking and harming is not the computer but the one which operating this.

Tomar, Rai, Kharb (2006) discussed about computer forensic the branch of science which deals with cyber-crimes and criminals. In present study , they focused about computer forensic science and their needs, cyber forensic tools, cyber laws and their limitations and daily challenges faced in computer forensic, They also discussed about some basics rules of cyber laws as mentioned in paper by author , Cyber laws have a vital job in characterizing the standards of cyber society, According to author electronic evidence plays vital role while serving as an evidence for the administrative purpose in the court of justice it continuous by following all the four basic procedure of forensic analysis that is collection, examination, analysis and reporting by improving the forensic technique as well as implementing more cyber laws it become easier to save the world from cyber-crimes.

Rao, Saini and Panda (2014) discussed about the consequence of cyber-crime on the economy of India, and how cyber-crimes are effecting economic growth. In present study a review was done with the objective of getting these outcomes utilizing poll as an instrument found that software piracy and pornography are the most common cyber-crimes in India. The main focus of author is to focus on the requirement of police having Central Computer Crime Response Wing for the purpose of serving and guiding both the state as well as other investigative agencies regarding computer crime investigation. The important statement stated by the author for the welfare of individual is that before proceeding any financial deal with the help of the internet, it is very necessary to search engine for the purpose of verifying the identity of an individual.

Sarmah, Sarmah and Baruh discussed about the human dependency on internet, crimes on internet and cyber laws which is responsible for maintaining a balance in cyber world. In present study they discussed about the history of the cyber-crimes and how cyber-crimes are getting evolved day by day. According to author Banking Malware, phone hijacking key logger are the most common type of Attacks from 2013 onwards, in paper author also provide some safety measures used in cyber space. They justified their work by discussing different case studies encountered in the same scenario. They also discussed about the awareness of cyber law to protect each and every one from cyber-crime and their impacts on world. Lastly, they also focused

Conclusion

In cyber-crime world India is 100% vulnerable because NIC (National Informatics Centre) of India is not able to provide India a secured email network most of the Govt. officials are using Gmail, Hotmail and many other email service providers a large amount of confidential data is stored in these service provider servers how can we say India is 100 % secure when this much amount of confidential information can be misused in many ways. According to **Tomar, Rai, Kharb in their work,** a model methodology is in progress in the Council of Europe including 41 nations to make a universal Convention on Cyber Crime. The Convention would address unlawful get to, illicit capture attempt, information impedance, framework obstruction, computer related fraud and computer related misrepresentation. Considering the information from the above discussed paper, there are several outcomes one can encountered while relating with the cyber-crime to cyber world.

On the other hand North Korea, USA, china and many other countries are using their brilliant mind in providing cyber security. The human factor is the biggest concern to cyber security, it is said that armature hacks system but professional's hacks peoples. It is way easier to corn peoples using social engineering techniques and make them reveal information rather using tools and technology, the final string is the weakest link happens to be our password (bank passwords, email passwords etc.). An analysis of 32 billion breached accounts indicates the simple thing that peoples are using insecure passwords and hackers have dictionary of passwords to launch brute force attacks. What is the actual future of cyber security if one had to portrait a picture of uncertainty in cyber space in cyber security, the world will leave with some hope? It is believe that people and technology can work together to find better solution. We have an amazing ability to sense, process and analyse huge amount of data with current computing power and big data analytics can do three things descriptive, predictive and prescriptive. But it is believe that humans are continue to evolve and adapt. We will learn to mitigate these threats and hopefully it will remain secure. At the end whatever technique we use to secure our networks it will be defeated in any time soon. This cycle keeps on running until meaning of security loses its worth..

References:

Allan Liska, and Timothy Gallo. OREILLY. O'Reilly Media, 2016, OREILLY, books.google.co.in.

Bhattacharyya, Dhruba K., and Jugal Kumar. Kalita. DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance. CRC Press/Taylor & Francis Group, 2016.

Cybercrime Survey Report - Assets.kpmg." KPMG, Dec. 2017, assets.kpmg/content/dam/kpmg/in/pdf/2017/12/Cyber-Crime-Survey.pdf.

Esther Ramdinmawii, et al. "International Journal of Web Technology." A Study on the Cyber-Crime and Cyber Criminals: A Global Problem, vol. 3, 3 June 2014, pp. 172–179., www.academia.edu.

Kharb, Dr. Latika. "International Journal of Engineering and Management Research." Cyber Crimes Becoming Threat to Cyber Security, vol. 7, no. 2, pp. 48–51., www.ijiris.com.

Maskun, et al. "Cyber Security: Rule of Use Internet Safely?" *Procedia - Social and Behavioral Sciences*, vol. 103, 2013, pp. 255–261., pdf.sciencedirectassets.com

P Tomar, et al. "The Internet Journal of Law, Healthcare and Ethics." New Vision of Computer Forensic Science: Need of Cyber Crime Law, vol. 4, 2006, pp. 1–6., print.ispub.com.

Rao, Yerra Shankar, et al. "International Journal for Research in Technological Studies| Vol. 1, Issue 10, September 2014 | ISSN (Online): 2348-1439." Effect of Cyber Crime Indian Economy, vol. 1, 1 Sept. 2014, pp. 4–7.

Reddy, K. Sambi. "International Journal of Innovative Research in Information Security (IJIRIS) ." *Cyber Crimes in India and the mechanism to prevent them*, vol. 3, no. 09, Dec. 2016, pp. 29–32., www.ijiris.com.

Sarmah, Animesh, et al. "A Brief Study on Cyber Crime and Cyber Law's of India." *International Research Journal of Engineering and Technology (IRJET)*, vol. 4, no. 6, 2017, pp. 1633–1640., www.irjet.net.

Shancang Li, and Li Da Xu. *SYNGRESS*. Todd Green, 2017, www.elsevier.com.