THINK INDIA JOURNAL

ISSN:0971-1260

Vol-22-Issue-36-December-2019

Study of Cyber Crimes Before & After Abrogation of Article 370, 35A in Jammu & Kashmir

Fatima Tamboli

Assistant Professor, Department of Computer Science, Sarhad College of Arts, Commerce & Science, Pune

ABSTRACT

Cyber crime is offence that can be carried out by using a computer, electronic device, computer network or other modes of information communication technology (ICT). This attack includes the spread of malware, viruses, hacking and denial of service attacks. The aim of this research paper to discuss following points: Cyber crime, types of cyber crime, prevention of cyber crime. In this paper I will describe how cyber attack in Jammu and Kashmir spread very fast after invalidate of article 370, 35A

Keywords: Cyber crime, Hacking, Virus, Security.

INTRODUCTION

Cyber crime occurs in cyberspace. It uses computer and internet. Cybercrime has severe peculiar impact on the individuals and society. Therefore, there is need to understand cybercrime in detail. There are several terms used to define cybercrime. The prior descriptions were "computer crime", "computer-related crime" or "crime by computer". With the common of digital field, a few new terms like "information-age" or "high-technology " crime were included to the cyber crime definition. Cyber crime is also referred as "net" crime, "digital", "electronic", "virtual", "IT", "High-tech" and Technology-enabled" crime. Cybercrime has three categories:

1. Target cybercrime: In this crime computer is target.

2. Tool cybercrime: The tool to perform crime is computer.

3. Computer incidental: Less use of computer to perform crime.

CLASSIFICATION OF CYBER CRIMES

Cybercrime is classified into following types.

1. Individual

2. Property

3. Government

In each category there are different methods and these methods vary from person to another.

1. **Individual -** This crime includes distributing pornography, cyber stalking, grooming and trafficking. This cybercrime is very serious.
2. **Property:** Criminal can commit stealing and robbing. Criminal can steal a person`s information like bank details, credit card details and misuse it to make online purchases; commit a scam to earn money; use malicious programs to gain access to an organization`s website or break the systems of the organization. These softwares can also harm software and hardware.
3. **Government:** This crime is not common. This crime is referred as cyber terrorism. This crime can create chaos and cause terror between the peaceful inhabitants. Criminals hack military websites, government websites. The criminal can be terrorist or hateful governments of other nations.

ISSN:0971-1260

Vol-22-Issue-36-December-2019

The different kinds of cybercrimes are

1. Unauthorized Access and Hacking: Unauthorized access means access of information, computer and network without the acknowledgement of the authorized person. An illegal interference into a computer, network is known as hacking. Every act committed to break a computer system or computer network is hacking. Hackers write different programs to corrupt the information on computer. They get kick out and personal financial gains from such attack.

Hackers steal the credit card information and use this information for transferring money from various bank accounts to their own account. Government websites are the most targeted sites for the hackers.

A hacker is an unauthorized user who attempts to access to an information system. Hacking is a crime. It is an attack in to the privacy of data. There are different classes of Hackers.

a) White Hat Hackers- White hat hacker shares information. They commit crime only for enjoyment.

b) Black Hat Hackers- They causes damage after invasion. They damage the system by stealing or modifying information or include worms or viruses. Black hat hackers are also called as crackers.

c) Grey Hat Hackers – Hacker hacks computer and computer networks for curiosity, challenge and sharing of information. They also steal or damage information.

2. Web Hijacking

Web hijacking refers to take control of other`s website. In web hijacking hacker modifies a web site contents without owner`s permission.

3. Pornography

Pornography means display of sexual acts. It also includes magazines, pornographic websites and the internet pornography which delivered over mobile phones.

4. Child Pornography

The Internet is used as a medium to sexually abuse children. The children are victim to the cybercrime. It includes sharing nude photographs of children, sexual chat with children.

5. Cyber Stalking

Cyber stalking is termed as harassment of victim by following them, making telephone calls, sending written messages. It may be followed by serious brutal acts such as physical harm to the victim.

Cyber stalking is repeated acts of dangerous behavior of the cybercriminal towards the victim. There are two categories of Stalkers online and offline.

6. Denial of service Attack

This attack is used to shut down a computer system or network, making it inaccessible to authorized users. DoS attack floods the machine, sends the requests to overload the system, create traffic in network that causes a crash. Popular flood attacks are Buffer overflow attacks, ICMP flood, SYN flood.

7. Virus Attacks

Viruses are the codes that have the potential to infect other programs and it also make copies of it and spread into other programs and softwares. Worms are the programs which spread from computer to computer and multiply like viruses. Worms attaches them to other software. Virus, worms, computer virus, Time bomb, slag code are the malicious. Viruses affect the information on a computer, either by deleting or altering it. On the opposite hand worms only make copies of them and do that repeatedly. Trojans are available at two sides, a Client side and a Server side. When the victim (unknowingly) runs the server on its machine, the attacker will then use the Client to attach to the Server and begin using the Trojan. Trojan uses TCP/IP and UDP protocol for communications.

8. Software Piracy

Software piracy is nothing but the stealing of genuine programs. This includes distributing, copying, selling or modifying the software. These quite crimes also include infringement of copyright, trademarks violations,

ISSN:0971-1260
Vol-22-Issue-36-December-2019

theft of computer ASCII text file, patent violations etc. Domain names also are trademarks and guarded by ICANN domain dispute resolution policy and also under trademark laws. Cyber squatters register name just like popular service provider name so on attract their users and obtain enjoy them.

9. Salami Attacks
The attack was committed for the commission of monetary crimes. Attacker forms the alteration so negligible that during a single case it might go completely unrecognized.

10. Phishing
In phishing attacker sends an e-mail to a user, access private information and used it for fraud.

The e-mail direct the users to go to an internet sites where they're asked to update their personal information, like credit card, passwords , Social Security. The online sites are bogus and created only to steal the user information.

Other cyber crimes are Sale of illegal articles, Online gambling, Email spoofing, Cyber Defamation, Forgery, Theft of data contained in electronic form, Email bombing, Internet time theft , Theft of computing system, Physically damaging a computing system, Violation of Confidentiality, Data diddling, Investment Frauds, Cyber Terrorism.

Growth rate of cyber crime in Jammu and Kashmir before and after abrogation of Article 370, 35A
The cyber crime in Jammu and Kashmir is noticing a sudden growth. In year 2017 total 51 such cases ware recorded within the state. According to figures in the year 2017, 51 cases of cyber crimes are witnessed in Jammu and Kashmir. In year 2015, there have been 38 cases associated with the cyber crime recorded within the state while as within the year 2016, the amount of such cases was 25. Cyber crimes noticed a sudden growth within the year 2017.

The government on floor of the house recently claimed that each one the Police Stations are given latest technologies and different IT Gadgets to handle Cyber Crimes. To tackle crimes within the Jammu and Kashmir government formed three Cyber Crime Police Cells at Jammu, Srinagar and Crime Headquarters with expert officers which monitor all cyber offences.

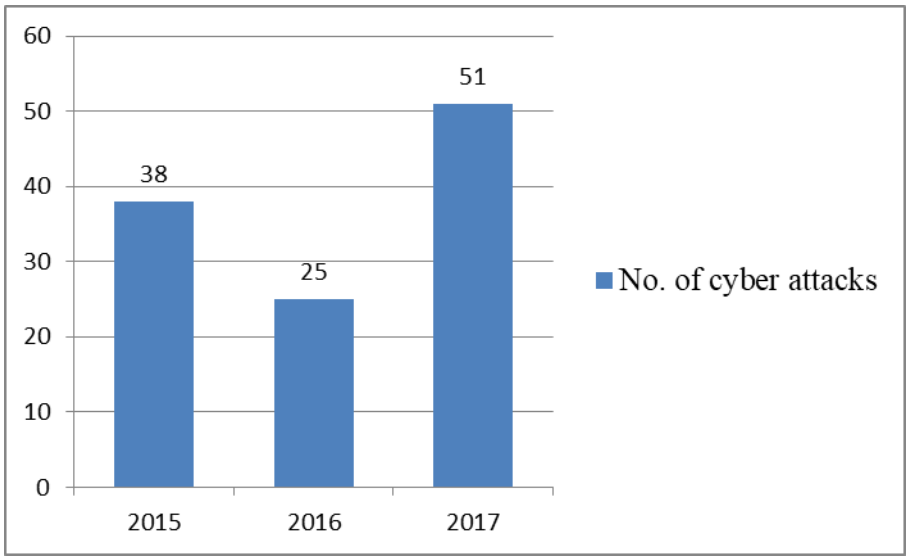

Figure-1: Year wise cyber attacks.

After the scrapping of Article 370 and 35A from J & K are witnessing a significant rise in cyber attacks that's affecting the critical infrastructure. According to report by IANS cyber-security Company Kaspersky has notified institutions to stay a strict check on its security. The official website of the Bihar Department of Education was hacked on 18th August by "RootAyyildiz Turkish Hacker", who has also claimed the responsibility for an equivalent. After hacking the web site he posted messages like "We Love Pakistan" on

ISSN:0971-1260

Vol-22-Issue-36-December-2019

the web site, Saurabh Sharma(Global Research and Analysis Team (GReAT) APAC, Kaspersky) said that they seen a rise in cyber-attacks after the abrogation of Article 370 by the Indian government. He also reveals that, as per Kaspersky's Cyberthreat World-time Map, India stands 7th among the foremost attacked countries within the world. 24 government's websites were hacked by hackers until May 2019(report by Indian Computer Emergency Response Team). IT Minister Shankar Prasad responded stating that attempts are made by hackers and cyber terrorists to launch cyber-attacks from variety of nations, including China and Pakistan. India experienced a rise in cyber attacks (20 percent report by IANS and Subex).

HOW TO PREVENT FROM CYBER CRIME

Prevention is usually better than cure. It's always better to require certain precautions while performing on internet. One should make them a neighborhood of his cyber life. Sailesh Kumar Zarkar, technical and network adviser from Mumbai Police Cybercrime Cell, recommends the 5P mantra for online security Prevention, Protection, Preservation, Precaution and Perseverance.

1. Provide education so cyber crime will be easily tackled.
2. Do not disclose any personal information to strangers, through e-mail or during chatting or any social networking site.
3. Do not send any photograph to strangers by online.
4. Update your Anti-virus software regularly to protect against virus attacks.
5. Do not share your credit card details on website.
6. Keep watch on websites which are accessed by children to avoid harassment.
7. Website owners should keep watch on traffic and any irregularity on the location
8. Use different security programs foe websites.
9. To prevent cyber crimes IT department should pass certain guidelines

CONCLUSION

Though not all people are victims to cyber crimes, they're still in danger. Cybercrimes became a true threat today and are quite different from regular crimes like stealing, mugging or robbing. Unlike these crimes, cybercrimes are often committed by single person and doesn't require the actual presence of the criminals. The crimes are often committed from a foreign location and therefore the criminals needn't worry about the enforcement agencies within the country where they're committing crimes. A cybercrime can play havoc in cyberspace if it's a bot attack. Because the speed of committing crime and impact is bigger in cybercrime cases and electronic evidence are often easily tampered it's imperative to trace the offender within the shortest possible time and preserve original evidence. Because the technology increases cyber attack also increases. After abrogation of Article 370, 35A in Jammu & Kashmir cyber attack increases.

REFERENCES

1. https://www.indiatimes.com/technology/news/india-is-getting-more-cyber- attacks-after-abrogation-of-article-370-35a-in-jammu-kashmir-373983.html
2. https://gadgets.ndtv.com/internet/news/india-sees-dramatic-rise-in-cyber-attacks-post-kashmir-decision-2087647
3. Cross Domain Solutions: Ensuring Complete Data Security; retrieved from http://www.crossdomainsolutions.com/cyber-crime/
4. Cyber Crimes: Law and Practice; retrieved from http://www.img.kerala.gov.in/docs/downloads/ cyber%20crimes.pdf
5. http://www.knskashmir.com/Cyber-Crimes-witness-surge-in-JK--51-cases- registered-in-2017-alone-23017.