Cyber Crime Evolved with Technology Evolution : case study

Dr. Yatu rani

CSE department
BMIET, sonipat
Haryana

Abstract: As all we know that technology is growing rapidly same as crime related to it increase as well. But here various questions arises that it is fault of technology or its fault of our careless attitude . Clearly we are connected over web which is look like a ocean. You meet various personality over there some of them are white hat and some of them are black hat wearer so Is not our responsibility to save our data from a stranger. We need to act more responsible.

Keywords: cyber crime, IT act, cyber attack,web wrongdoing

INTRODUCTION

Crime is a major and legal problem in the world we live in and population is one of important factor, which influencing incidence of crime. Currently cyber crimes increasing very fast as technology is growing very rapidly.so its difficult to investigate without a proper framework. Cyber crime includes all the crimes or offences that include use of computers or associated electronic devices. Its not limited to mail ,google but also include social networking, banking and shopping sites. Computer crime define as criminal activity involving an information technology infrastructure, including illegal access,illegal interception,misuse of devices,frogery and electronic fraud.By getting cyber space its rapidly increment in sort of activity which are prohibited by law wheather national or international.A legal framework for cyber world was conceived In India in the form of E-commerce act,1998.

Afterwards the basic law for cyberspace transactions in india has emerged in form of information technology act,2000 which amended in year 2008.but till date its more on paper than execuation.because lack of understanding for its highly technical terminology.

The major international organizations like OECD and G-8 areseriously disscusing cooperative scheme but some countries do not share combat cyber crime.

We are living in digital era where technologies are retouched and proliferate rapidly day by day because of this whole society in fence with gadgets .Criminals are also encourage by technologies and crime is converted into cybercrime with the assistance of computers (Desktops), laptops, mobile phones, etc. To quest criminals and to get rid of cybercrime, a new branch of forensic science is introduced which Digital forensic science is thus encompassing the investigation, track evidence with the help of electronic media and recovery of materials found on digital devices. The nature of crime is still same but the way has changed completely now criminals are using technology to get close to victims instead of going in victims place. In this paper we will discuss about what is cybercrime, explore different categories of cyber-attacks, the Deep web and who digital forensic helps in detection and controlling in cybercrimes. We conclude our study by analyzing some modification required in present digital forensic model and proposed future actions that should be taken to tackle cyber-crime and harden cyber security.

Case study of cyber crime cases(India region only)

Case 1 SIM Swap Fraud

In August 2018, two men from Mumbai were arrested for cybercrime. They were involved in fraudulent activities concerning money transfers from the bank accounts of numerous individuals by getting their SIM card information through illegal means. These fraudsters were getting the details of people and were later blocking their SIM Cards with the help of fake documents post which they were carrying out transactions through online banking. They were accused of transferring 4 crore Indian Rupees effectively from various accounts. They even tried to hack the accounts of a couple of companies. In this, the fraudsters will get the information of the customers like their phone number, name, id proof and so many from an organization or from some public domains. After that, they were getting the 4G sim card by producing the required information of customers who uses 3G sim card with their phone numbers to the telecom company and call the customer and act as a customer service executive. They will give 20-digit number which will be written at the back side of 4G sim card and ask the customer key in and activate the 4G sim card easily. When customers do that, the 3G sim card will be deactivated and 4G sim card will be activated. But 4G sim card is still with the fraudsters in which they will perform bank transactions and receive OTPs.

Case 2 Cyber Attack on Cosmos Bank

A daring cyber-attack was carried in August 2018 on Cosmos Bank's Pune branch which saw nearly 94 Crores rupees being siphoned off. Hackers wiped out money and transferred it to a bank which is situated in Hong Kong by hacking the server of Cosmos Bank. A case was filed by Cosmos bank with Pune cyber cell for the cyber-attack. Hackers hacked into the ATM server of the bank and stole details of many visa and rupay debit cards owners. The attack was not on centralized banking solution of Cosmos bank. The balances and total accounts statistics remained unchanged and there was no effect on the bank account of holders. The switching system which acts as an interacting module between the payment gateways and the bank's centralized banking solution was attacked. The Malware attack on the switching system raised numerous wrong messages confirming various demands of payment of visa and rupay debit card internationally. The total transactions were 14,000 in numbers with over 450 cards across 28 countries. On the national level, it has been done through 400 cards and the transactions

involved were 2,800. This was the first malware attack in India against the switching system which broke the communication between the payment gateway and the bank

Case 3 Stealing of Credit and Debit Card Information

In 2007 three men have been indicted for hacking into cash registers machine at Dave & Buster's restaurant locations in the US stealing data from thousands of credit and debit cards. That data that was later sold and caused more than $600,000 in losses. One from Ukraine and other from Estonia hacked into cash register machines at 11 Dave & Buster's locations and installed "sniffer" programs to steal payment data as it was being transmitted from the point-of-sale terminals to the company's corporate offices. Later the same men were charged with similar a breach at TJMax. Some Analysts estimated the losses at TJ Max at more than USD$1 Billion [7]. An inspector with the U.S. Postal Inspection Service alleged one of the three men was a major reseller of stolen credentials [7]. Notably all the three men were arrested while visiting two countries, which actively co-operate with US law enforcement Turkey and Germany and not at home in Eastern Europe.

Case 4 Hacking the Websites :

Over 22,000 websites were hacked between the months of April 2017 and January 2018. As per the information presented by the Indian Computer Emergency Response Team, over 493 websites were affected by malware propagation including 114 websites run by the government. The attacks were intended to gather information about the services and details of the users in their network.

Case 5 ATM System Hacked in Kolkata

In July 2018 fraudsters hacked into Canara bank ATM servers and wiped off almost 20 lakh rupees from different bank accounts. The number of victims was over 50 and it was believed that they were holding the account details of more than 300 ATM users across India. The hackers used skimming devices on ATMs to steal the information of debit card holders and made a minimum transaction of INR 10,000 and the maximum of INR 40,000 per account. On 5 August 2018, two men were arrested in New Delhi who was working with an international gang that uses skimming activities to extract the details of bank account.

Conclusion

Cyber Crime which is otherwise called * Web wrongdoings' or PC violations is any crime that uses a PC either an instrument, target or a methodsfor propagating furtherwrongdoings or offensesor negations under any fa, Cybercrime is by and largeviewedas any criminalbehaviordirectedthrougha PC. The stress is bercrimeas a noteworthy worry to the worldwide network.Makingmindfulness on digitalsecurityissuesis onificant for Malaysians as Malaysians viewedas an advancing countryin the field of innovation. Thus, the cybercrime activities will be increasing in the upcoming days and will not be stopped. So, a better approach to stop this cybercrime is to build a powerful system which can stop this kind of crimes by comprising of powerful firewall, IDS, SDN Controller and maintenance should be done periodically. Also, the protection for the customer's data should be given higher priority and place it confidentially with high privacy. The conclusion of this literature review is that the data is so much important now a days as it can be used to earn huge amount of money

Thepresentation,development,and use of data and correspondence advances(ICTs)have been joinedby an expansion in crimes. There are four noteworthy classifications of digitalviolations such a digitalwrongdoing againstpeople,digitalwrongdoing againstproperty, digitalwrongdoing againstassociationand digital wrongdoing againstsoCiety.Digitalviolations againstpeopleare hacking.emailsatirizing.spamming.digitai criticism and provocation, digitalstalkingand digitalharassing. "Hacking in laymantermsimpliesan unlawful interruption into a PC framework".

The characteristic idea of the web crushes every physical limit and hence turns into a universal system of data frameworks, servings wide range of capacities, be they open or private,benetitmakingor basically the unnecessary spread of data. The utilization of data and correspondence advances(ICTs)is continually extending, with the quantity of clientsdevelopingexponentiallyeveryyear.Somewhere in the range of 2000 and 2005, the normal web client development rate was of 146.2 percent,the most elevatedrate being in the Middle East with 266.5 percent.Not a long ways behind were Latin America and the Caribbean with 211.2 percent and Asia with 198.3 per cent. It is obviousfrom theseinsightsthat theseareas,wheremost aerating nationssubsist,are anxious executant abuse the upsidesof lCTs and the web superhighway.

REFERENCES

1. Shamti Sarkhel,A Study on ExistingAgileMethods,GlobusAn InternationalJournal of Management & . IT, Vol 7, No 1, 2015.
2. Pegu, Shemantaand Sharma,Dr. A.K., "A Study of E-Commerce in Modernization of Indian Libraries". . Globus Journalof Progressive Education, 5 (1): 1-3, 2015.
3. Perrig."Practical techniques for searchesin encrypted data," in IEEE Sym. On Researchin Security and 8. Privacy,vol.33,issue35, pp.678-687, 2013.
4. PricewaterhouseCoopers (PwC) "Economic Crime Survey India Report, 2011
5. Vangie Beal "definition of Cyber-crime". Retrieved 24th October 2015, http://www.webopedia.com /TERM/C/cyber_crime.html
6. KPMG in India, Cybercrime survey report, 2014
7. Yu, H., Hou, S., & Lang, L. (2018). The Exploration of Historical Blocks' Protection and Renovation Based on the Theory of City Image. Current Urban Studies, 06(03), 425–432. https://doi.org/10.4236/cus.2018.63023 [8
8. Testybytes.in (2018). Major Cyber Attacks on India (2018) – Testbytes. Retrieved August 23, 2018, from https://www.testbytes.net/blog/cyber-attacks-on-india-2018/
9. Nohe, P. (2018). 2018 Cybercrime Statistics: A closer look at the Web of Profit. Retrieved from https://www.thesslstore.com/blog/2018-cybercrime-statistics/
10. CERT, K. L. I. (2019). Kaspersky Lab ICS CERT _ Kaspersky Lab Industrial Control Systems Cyber Emergency Response Team. Retrieved September 20, 2001, from https://ics-cert.kaspersky.com/