Volume 6, Issue 5, May 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Cyber Crime-Its Types, Analysis and Prevention Techniques

[1]Alpna, [2]Dr. Sona Malhotra
[1] Mtech Student, [2] Assistant Professor
[1, 2,] University Institute of Engineering and Technology, Kurukshetra University, Kurukshetra, Haryana India

Abstract: The user of computer system and internet are increasing worldwide in large number day by day, where it is easy to access any information easily within a few seconds by using internet which is the medium for huge information and a base of communications around the world .There has been tremendous growth in use of Internet. Due to this cyber crimes increases day by day. Cyber Crime is technology based crime committed by technocrats. This paper deals with Variants of cyber crime like terrorist attack, cyber extortion, crimes against individuals, crimes against property, and crimes against organization. It also includes impact on the real world and society, and how to handle cyber crimes.

Keywords: cyber crime, types of cyber crime, case study, prevention methods for cyber crimes, graph analysis.

I. INTRODUCTION

In today's world, an organization dependency on cyberspace is becoming an increasingly aspect of organizational security. The infrastructure of different organizations are interconnected in cyberspace, therefore the level of risk to security has increased dramatically. The threat to cyber security is growing at vast rate. Computer systems at colleges and Universities have become targets as they store same record as bank. The cyber crimes involve the use of computer, internet, cyberspace and the World Wide Web and give rise to the criminal activities. Cyber criminals are becoming more Sophisticated and are targeting consumers as well as public and private organizations. Cyber crimes are rises due to the lack of cyber security.

All types of cyber crimes consist of both the computer and the person behind it as victims. Cyber crime could include anything such as downloading

Illegal music files to stealing millions of dollars from online bank accounts. Cyber crime could also creating and distributing small or large programs written by programmers called viruses on other computers or posting confidential business information on the Internet to harm the peoples. An important form of cyber crime is identity theft, in which criminals use the Internet to steal personal information from other users.

An example of one type of cyber crime is an *account takeover*. An incident occurred in 2012 at the South Carolina 'Department of Revenue' that illustrates this cybercrime. Cybercriminals broke into the department's computer systems and stole 3.6 million Social Security numbers and 387,000 credit/debit card numbers this happens when cyber criminals compromise your computer and install malicious software, such as *key loggers*, which record key strokes, passwords, and other private information. This in turn allows them access to programs and web sites using your log-in credentials. Once these criminals steal your password, they may be able to breach your online bank account. These criminals can be anywhere in the world and may be able to transfer your money almost immediately. [6]

II. DIFFERENT TYPES OF CYBER ATTACKS:

1) Cyber crime against individual

*i) E-Mail Spoofing***:** this means a spoofed email is one that appears to originate from one source but actually has been sent from another source. This can also be termed as E-Mail forging. The main goal of the attacker in this case is to interrupt the victim's e-mail service by sending him a large number of emails.

ii) Phishing: Phishing means trying to fool people into parting with their money. Phishing refers to the receipt of unsolicited emails by customers of financial institutions, requesting them to enter their username, password or other personal information to access their account. The criminal then has access to the customer's online bank account and to the funds contained in that account. The customers click on the links on the email to enter their information, and so they remain unaware that the fraud has occurred

iii) Spamming: Spam is the abuse of electronic messaging system to send unsolicited bulk messages indiscriminately

iv) *Cyber defamation*: It involves any person with intent to lower down the dignity/image of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.

v) Cyber stalking and harassment: The use of Internet to repeatedly harass another person group, or organization. This harassment could be sexual in nature, or it could have other motivations including anger.

vi) Computer sabotage: the use of the internet to halt the normal functioning of a computer system through the introduction of worms, viruses, or logic bomb is referred to as computer sabotage.

vii) *Malware*: Malware is any software that infects and damages a computer system without the owner's knowledge or permission and takes control of any individual's computer to spread a bug to other people's devices or social networking profiles. Such software can also be used to create a 'botnet'— a network of computers controlled remotely by hacker to spread spam or viruses.

2) Crime against property

*i) Intellectual Property Crimes***:** Any unlawful act by which the owner is deprived completely or partially of his rights is a crime. The most common type of crimes are software piracy, infringement of copyright, trademark , theft of computer source code, etc.

*ii)Cyber Squatting***:** It involves two persons claiming for the same Domain Name either by claiming that they had registered the name first. For example two similar names i.e. www.yahoo.com and www.yahhoo.com.

*iii) Cyber Vandalism***:** Vandalism means damaging property of another. Thus cyber vandalism means destroying or damaging the data or information stored in computer when a network service is stopped or disrupted.

iv) *Hacking Computer System***:** Hacking in simple terms means an" illegal intrusion into a computer system and/or network". Hacking attacks include Famous social networking sites such as facebook, Twitter, blogging platform by unauthorized access/control over the computer. Due to the hacking activity there will be loss of data as well as computer system. Also research especially indicates that those attacks were not mainly intended for financial gain too and to diminish the reputation of particular person or company.

v) Altering in an unauthorized way. This requires little technical expertise and is common form of theft by employees altering the data before entry or entering false data, or by entering unauthorized instructions or using unauthorized processes;

Altering, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions.

3) Cyber crime against organization

*i)Hacking***:** It means unauthorized control/access over computer system and act of hacking completely destroys the whole data as well as computer programs.

ii) Password sniffing: password sniffers are programs that monitor and record the name and password of network users as they login, at site.

iii) Denial of service attacks: the criminal floods the bandwidth of the victim's network. The attackers typically target site or service hosted on high-profile web servers such as bank, credit card payment gateways, mobile phone networks and even root name servers.

Denial of service attacks are designed to consume resources so that other users are unable to use the resources and are therefore "denied service". In a Computer network environment, the key resources are CPU, memory, and bandwidth

iv) Virus attack: A computer virus is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected.

V) E-mail bombing/mail bomb: refers to sending a large no of emails to the victim to crash victim's E-mail account or server crash.

vi) Salami attack: these attacks used for committing financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed e.g. a bank employee inserts a program into bank's servers that deducts a small amount from the account of every customer.

Vii) Logic bomb: A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are available. For example, a programmer may hide a piece of code that starts deleting files should they ever be terminated from the company.

viii) Trojan horse: Trojan horses are email viruses that can duplicate themselves, steal information, or harm the computer system.

III. CASE STUDY

CASE 1

THEFT OF SENSITIVE DATA: An incident occurred in 2012 at the South Carolina 'Department of Revenue' that illustrates this cybercrime. Cybercriminals broke into the department's computer systems and stole 3.6 million Social Security numbers and 387,000 credit/debit card numbers

Cause

i) The crime occurs when a cybercriminal gains access to sensitive data and steals it. The crime can be as simple as copying an entity's customer data files onto a flash drive and selling it to a competitor, or using confidential or proprietary information to compete with the entity's business.

ii) According to investigation report at least one employee felt for the trick and opened the file, which infected the computer

iii) Its malware had key logging capabilities to intercept the employee's name and password

Weak security cause:

i) The workers were not required to use multiple passwords when trying to obtain sensitive information and the state also did not encrypt sensitive data lack of encryption.

ii)It all began the malicious email sent to multiple employees , which eventually resulted in 44 systems used 33 pieces of malicious s/w and utilities , remotely accessed revenue dept servers from at least 4 valid dept accounts to carry their activities

iii) After stealing login credentials the attacker used the legitimate user data to use the "CRITIX REMOTE ACCESS" service. The attacker use critix portal to log into the user work station and escalated privileges in order to access other system and database on n/w. the attacker harvested account password on six different servers, executed and utility to steal passwords for windows use and open backdoor to compromised machinery account

Impact: Hackers got access to data on 3.3 million bank account and 699900 business tax returns

CASE 2

CYBER EXTORTION: "THE SONY PICTURES ENTERTAINMENT" hack was a release of confidential data belonging to Sony Pictures Entertainment on November 24, 2014. The data included personal information about Sony Pictures employees and their families, e-mails between employees, information about executive salaries at the company, copies of (previously) unreleased Sony films, and other information. The hackers called themselves the "Guardians of Peace" or "GOP"

Cause

i) A malware software program designed to erase the data from servers. The malware previously installed rendered many SONY employees computer in coperable by the s/w with warning by the guardians of peace , along with a portion of the confidential data taken during the hack

ii)"HEARTBLEED" a bug discovered which allowed hackers to attack two third of web servers that used open source SSL security certificates. Open source SSL is a piece of cryptographic program which is utilized across the web to protect our communication and identities. Not only did the bug made comm. Vulnerable , it also forced server to leak sensitive data including passwords, private cryptographic keys among other from memory

iii)"RANSOMWARE" one of the type of malicious s/w , it locks up all the personal documents and files the victim computer and demands payment in exchange of regaining access.

Weak security causes: Lack of monitoring, Minimal backup and failover capabilities, Antivirus s/w fails to identify malware due to archaic signature based model they used.

Impact: $15 million harm to economy, theft of 77 million play station , Sony pictures went down for 2 days forcing employees to work at home and use paper and pencil to do their work , every pc in the company is useless .

CASE 3

Terrorist attack: The first "hacktivist" (hacking activist) attack, the WANK worm hit NASA offices in Greenbelt, Maryland. WANK (Worms against Nuclear Killers) ran a banner (pictured) across system computers as part of a protest to stop the launch of the plutonium-fueled, Jupiter-bound Galileo probe. Cleaning up after the crack has been said to have cost NASA up to a half of a million dollars in time and resources Melbourne-based hackers, Electron and Phoenix

Cause: The worm coincidentally appeared on the DEC.net computer network shared between NASA and USA dept on energy before the launch of NASA space shuttle. The worm propagated through the n/w pseudo randomly from one system to another by using the algorithm which converted the victim's machine system time to candidate target node address and subsequently attempt to exploit weakly secured system

Impact: More than 1.2 million dollar damage

CASE 4

The July 2009 cyber attacks were a series of coordinated cyber attack against major government, news media, and financial websites in South Korea and the United States

Cause

i) The attacks involved the activation of a Botnet—a large number of hijacked computers—that maliciously accessed targeted websites with the intention of causing their servers to overload due to the influx of traffic, known as a D DoS attack .Most of the hijacked computers were located in South Korea.

ii)The culprit is a piece of malicious s/w that order infected PC to visit the websites on its hit list over and over again, all in apparent bid to render the target unreachable to

Legitimate visitors

iii) Malware carried the cryptic message "get/china/dns.

iv) Malicious code responsible for causing the attack identified as "W32.DOZER" is programmed to destroy data on infected computers and prevent the computers from rebooted

v) Security experts say that the attack reused code from the "Mydoom Woom".

Weak security causes: Financial sector passwords are considered weak, Peer to peer file sharing system weak

Impact: the attacks have targeted major public and private sector websites, the South Korean Presidential office the data generated by the attacking program appeared to be based on a Korean-language browse

CASE 5

CYBER TERRORIST ATTACK: MUMBAI ATTACK 26/11

i) Mumbai attacks were planned and directed by Lashkar-e-Taiba militants inside Pakistan, and carried out by 10 young armed men trained and sent to Mumbai and directed from inside Pakistan via mobile phones and VoIP

ii)Eight of the attacks occurred in South Mumbai at Chhatrapati Shivaji Terminus, the Oberoi Trident, the Taj Mahal Palace & Tower, Leopold Cafe, Cama Hospital, the Nariman House Jewish community centre the Metro Cinema, and in a lane behind the *Times of India* building and St. Xavier's College

Technical cause

i) Cyber technology has played a role in this crime All the 26/11 planning mission was done via" GOOGLE MAP". The terrorists used cellular phone networks as command and control and social media to track and thwart the efforts of Indian commandos.

ii) The Pakistan's lashkar-e-toiba had used voice over internet protocol s/w to communicate with 26/11 attackers on the ground and direct the large scale operations on a real time basis

iii) The report claimed that the attacks unfold live on the television were inform the attackers of movement of security forces from news accounts and provide instructions

iv) The feature of VIOP based communication which form the technical basis of popular communication software such as SKYPE, VONAGE is that audio signals that convert the data and travel through most the internet infrastructure in binary , rather than audio format

*Weak security causes***:** Failure of SPY agencies – US, British, India

IV. PREVENTION METHODS FOR CYBER CRIME

1)**.** *Use strong passwords*.

i) Use separate ID/password combinations for different accounts, and avoid writing them down.

ii) Make the passwords more complicated by combining letters, numbers, and special characters. Change them on a regular basis.

iii) Use strong passwords with upper case, lower case, number and special characters and minimum of 6 characters.

iv) Don't use passwords that contain names, birthdays, phone numbers, etc.

v) Don't share passwords across multiple services i.e. same password for Gmail, Credit Cards, Work, Twitter, etc.

vi) Don't use sequential passwords for different services i.e. ABC10, ABC11, ABC12, etc.

vii) Don't store your passwords under your keyboard, in your drawer, in Outlook, Gmail, Phone, password wallet software, etc.

viii) Best place to store passwords is in your brain; second best is written on a piece of paper and kept in your wallet.

ix) Never tell your password to anyone, including people from support, customer service, helpdesk, etc.

2). *Secure your computer*:

i) Enable your firewall: Firewalls are the first line of cyber defense; they block connections from suspicious traffic and keep out some types of viruses and hackers

ii) Use anti-virus/malware software: Prevent viruses from infecting your computer by installing and regularly updating anti-virus software.

3). *Block spyware attacks*. Prevent spyware from infiltrating your computer by installing and updating anti-spyware software.

4). *Install the latest operating system updates*: Keep your applications and operating system (e.g., Windows, Mac, Linux) current with the latest system updates. Turn on automatic updates to prevent potential attacks on older software.

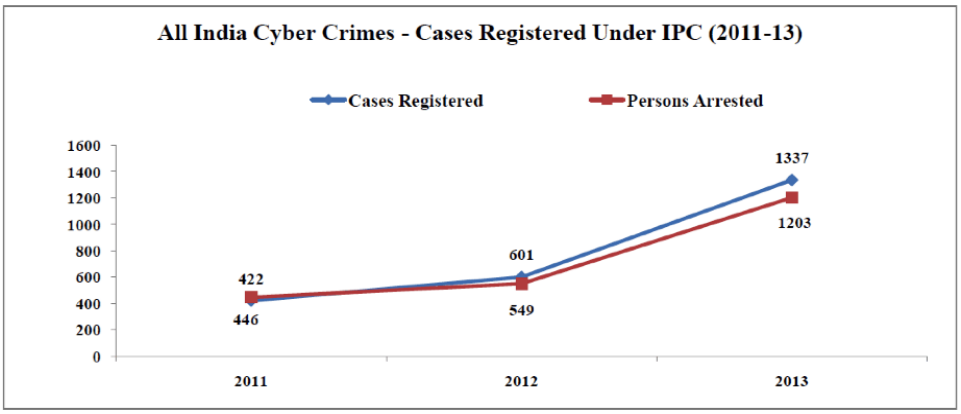
5). *Protect your data*: Use encryption for your most sensitive files such as health records, tax returns, and financial records. Make regular backups of all of your important data.

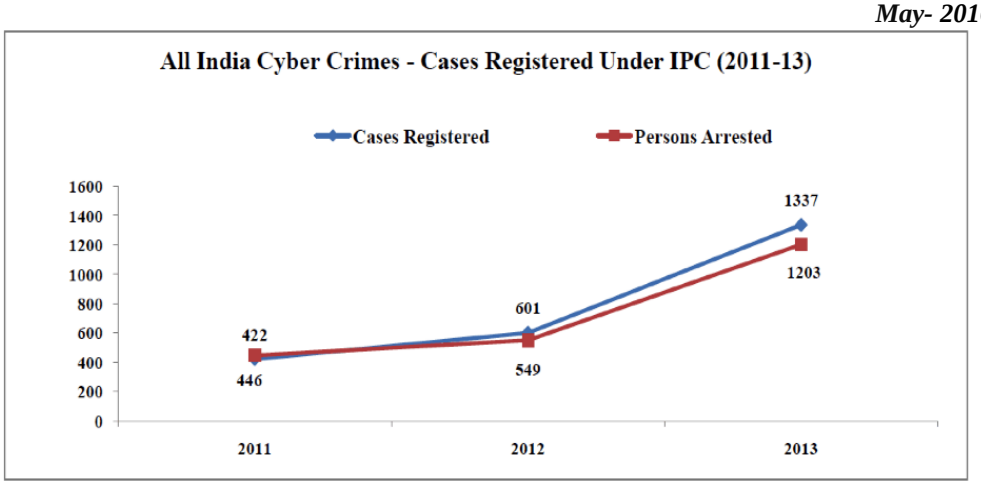
6). *Secure your wireless network*: Wi-Fi (wireless) networks are vulnerable to intrusion if they are not properly secured.

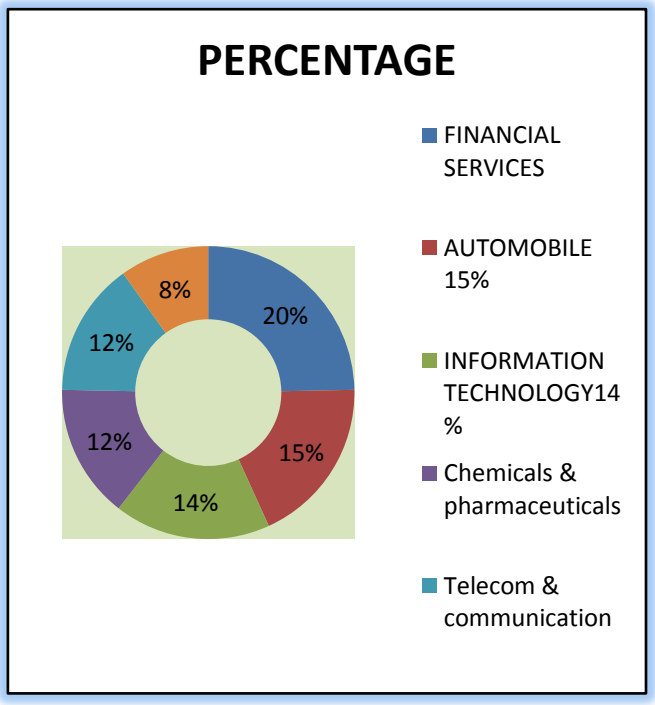
7). *protect your e-identity*: Be cautious when giving out personal information such as your name, address, phone number, or financial information on the Internet. Ensure that websites are secure, especially when making online purchases, or ensure that you've enabled privacy settings (e.g., when accessing/using social networking sites, such as Facebook, Twitter, YouTube, etc.). Once something is posted on the Internet, it may be there forever.

8). *Avoid being scammed*: Never reply to emails that ask you to verify your information or confirm your user ID or password. Don't click on a link or file of unknown origin. Check the source of the message; when in doubt, verify the source.

V. GRAPH ANALYSIS







Source: Cybercrime survey report 2014, KPMG in India [11]
(Affected areas due to cyber crime)

VI. CONCLUSION

Computer crime does have a drastic effect on the world in which we live. It affects every person no matter where they are from. This paper discussed different type's cyber attacks. Cyber attack techniques have been improved dramatically over time, especially in the past few years. Criminals have also adapted the advancements of computer technology to further their own illegal activities. Certain precautionary measures should be taken by all of us while using the internet which will assist in challenging this major threat Cyber Crime. There is a need to conduct research analysis of cyber crimes to find out a best approach to protect sensitive data and take appropriate action against the cyber attack.

ACKNOWLEDGEMENT

The satisfaction that accompanies the successful completion of any task would be incomplete without the mention of people whose cooperation made it possible, whose constant guidance and encouragement crown all efforts with success. I own my regards *to Dr. Sona Malhotra(ASTT PROFFESOR UIET KURUKSHETRA,KURUKSHETRA UNIVERSITY)* my Guide, for reviewing, advising, suggestion, motivation and extended keen interest.

REFERENCES

[1] Vineet Kandpal and **R. K. Singh, *Latest Face of Cybercrime and Its Prevention In India*, International Journal of Basic and Applied Sciences Vol. 2. No. 4. 2013

[2] Er. Harpreet Singh Dalla, Ms. Geeta HOD, Department of CSE & IT Patiala Institute of Engineering & Technology for Women, Patiala, *India, Cyber Crime – A Threat to Persons, Property*, Government and Societies, Volume 3, Issue 5, May 2013 ISSN: 2277 128X

[3] Jamal Raiyn, *A survey of Cyber Attack Detection Strategies*, International Journal of Security and Its Applications Vol.8, No.1 (2014).

[4] Angel cruz,chief information security officer state of Texas, cyber security tips, monthly newsletter 2013,volume

[5] Atul M. Tonge1, Suraj S. Kasture2, Surbhi R. Chaudhari3 IOSR Journal of Computer Engineering (IOSR-JCE) CSE, *Cyber security*: *challenges for society*,ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 2 (May. - Jun. 2013).

[6] Forensic technology services cybercrime survey report 2014 kpmg.com/in

[7] Atul Kum ar, Sr. Analyst, Chiranshu Ahuja, Sr. Analyst, *Cyber Security Research Developments Global and Indian Context*, A NASSCOM® Initiative

[8] Sumanjit Das and Tapaswini Nayak, *"impact of cyber crime: issues and challenges*", International Journal of Engineering Sciences & Emerging Technologies, October 2013. ISSN: 22316604 Volume 6, Issue 2, pp: 142-153 ©IJESET.

[9] Janhavi J Deshmukh and Surbhi R Chaudhari, *Cyber crime in Indian scenario – a literature snapshot*, International Journal of Conceptions on Computing and Information Technology Vol.2, Issue 2, April' 2014; ISSN: 2345 – 9808.

[10] https://factly.in/cyber-crimes-in-india-which-state-tops-the-chart.

[11] Cybercrime survey report 2014, KPMG in India.

