Information about Cyber Crimes and Cyber Security: With Solutions

P.NITHIN KUMAR REDDY, K.HEMANTH, V HARSHA VARDHAN

Abstract—The rapid technological developments, our life is becoming more digitalized. Be it business, education, shopping or banking transactions everything is on the cyber space. There are some threats posed by this incredible rise in digitization which is creating a new set of global concern called as cyber crime. It is easy to fall prey to such unethical way of hacking and penetrating into personal life which is feasible at a click of a button. Cyber crimes 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. This paper identifies the importance of being acquainted with the effects of cyber crime keeping in mind the recent activities that have taken place and offering solutions to protect oneself from it. Moreover, highlighting the need of being cyber safe and how such illegal activities can be a problem for us. The present paper reviews the current solutions to deal with the alarming rise in these criminal activities. Hi-tech technologies that need to be adopted to prevent oneself from getting webbed have been recommended in the paper. A few case studies have been discussed and innovative suggestions for future cyber security proposed.

Key words— Cyber Crime, Information Security, Cyber threats, Hacking, Phishing, Cyber Safety, Digital Data.

—————————— ◆ ——————————

1 INTRODUCTION

Cyber Crimes relates to the word cyber which encompasses the computer network, using which one can perform any activity in the real time world. Cyber Crimes such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy use digital data from Computer systems and other electronic devices. These devices are used as a target by attacking the computer through viruses, as a weapon to commit crimes or as an accessory to store illegal information. Cyber Crimes also affect business every year, losing billions of money and damaging the company's reputations leading to loss of future business as well. In today's world, cyber systems provide flexibility leading to its illicit use. With the Government framed Internet policy, Internet along with making the life easy with economic activities like buying, selling, online transactions and social networking brings along many threats. Hacking tools are available on the internet which does not require people to be highly skilled and also encourage them to do inappropriate acts online. Thus, cyber space has made users vulnerable making it important to take necessary steps and avoid exposure from to acts. Highly populated countries like Asia, China are dependant on web resources which creates opportunity to commit such crimes and also makes it difficult to detect and prevent Internet Crimes in the wide networking environment.

2 INFORMATION ABOUT CYBER CRIME:

2.1) There are a lot of cases of Computer Assisted crime where computer is the instrument for committing crime. Some of them are discussed below:

2.1.1) Data Piracy: Data piracy is reproduction of digital data and easy distribution of print, graphics, sound and different types of data which will be used by others illegally.

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

2.1.3) Illegal Interception of Material: Data transfer over the net has resulted in greater speed and capacity but also greater vulnerability. It is now easier for unauthorized people to gain access to sensitive information. It has many forms like:

————————————————

- *P Nithin Kumar Reddy is currently pursuing Master of Computer Applications in KMM Institute of PG studies in S.V University, Andhra pradesh, PH-9966723273. E-mail: nitin.nhn333@gmail.com@gmail.com*
- *K. Hemanth kumar is currently pursuing Master of Computer Applications in KMM Institute of PG studies in S.V University, Andhra pradesh, PH-7794923947. E-mail: kumar11.hemanth@gmail.com.*
- *Vemuri Harsha vardhan is currently working as Assistant Professor in KMM Institute of PG studies in S.V University, Andhra pradesh, PH-9959974091.
E-mail: vemuriharsha@gmail.com*

2.1.3.1) Online Credit card fraud, E- Bank theft: Illegal acquisition of credit card number for online purchases or bank account details where the perpetrator diverts funds to account accessible to criminal.

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

2.2.1) Hacking: Information theft from computer storage device or hard disk and stealing username, password and altering information is called hacking.

2.2.2) Forgery: It includes reproduction of documents, certificates, identity thefts and fake currency.

2.2.3) Altering Websites: Here the hacker deletes some pages of a website, uploads new pages with the similar name and controls the messages conveyed by the web site.

2.2.4) Cyber terrorism: It involves E-murder or homicide or suicide or Spyware.

3 HOW CYBER CRIME WILL PERFORM

HACKING:- Hacking involves gaining unauthorized access to a computer and altering the system in such a way as to permit continued access, along with changing the configuration, purpose, or operation of the target machine, all without the knowledge or approval of the systems owners.

DENIAL OF SERVICE ATTACK: - A Denial of Service (“DoS”) attack is a rather primitive technique that overwhelms the resources of the target computer which results in the denial of server access to other computers. There are several different techniques that hackers use to “bring down” a server. As the network administrators learn how to limit the damage of one technique, hackers often create more powerful and more sophisticated techniques that force system administrators to continually react against assaults. In order to understand how to apply the law to these attacks, a basic understanding of the anatomy of the attacks is necessary This is an act by the criminal,, who floods the bandwidth of the victim’s network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide

Why do people Create These Viruses?

- **To distribute political message.**
- **To attack the products of specific companies.**
- **Some consider their creations to be works of art, and see as a creative hobby.**
- **Financial gain from identity theft.**

CREDIT CARD FRAUD:- Intangible assets represented in data format such as money on deposits or hours of work are the most common targets related to fraud. Modern business is quickly replacing cash with deposits transacted on computer system creating computer fraud. Credit card information as well as personal and financial information on credit card has been frequently targeted by organized criminal crimes. Assets represented in data format often have a considerably higher value than traditionally economic assets resulting in potentially greater economic class.

Internet time thefts: Phishing, spoofing or spam and different things were sends fictitious mails which appears official causing the victim to release personal information. The thefts were as follows as:

PHISHING:- Phishing, the mass distribution of “spoofed” e-mail messages, which appear to come from banks, insurance agencies, retailers or credit card companies and are designed to fool recipients into divulging personal data such as account names, passwords, or credit card numbers.

SPOOFIN:- Getting one computer on a network to pretend to have the identity of another computer, usually one with special access Privileges , so as to obtain access to the other computers on the network.

CYBER STALKING:- The Criminal follows the victim by sending emails,, entering the chat rooms frequently. In order to harass a women her telephone number is given to others as if she wants to befriend males befriend males.

THREATENING:- The Criminal sends threatening email or comes in contact in chat rooms with Victim.

3 CAUSES OF CYBER CRIMES

3.1) ***Ease of access:*** The problem encountered in guarding a computer system from unauthorised access is that there is every possibility of violating the technology by stealing 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.

3.2) Cyber Hoaxes: Cyber Crimes can be committed just to cause threats or damage one's reputation. This is the most dangerous of all causes. The involved believe in fighting their cause and want their goal to be achieved. They are called cyber terrorists.

3.3) ***Negligence*****:** There are possibilities of not paying attention in protecting the system. This negligence gives the criminals control to damage the computer.

3.4) Revenge or Motivation: The greed to master the complex system with a desire to inflict loss to the victim. This includes youngsters or those who are driven by lust to make quick money and they tamper with data like e-commerce, e-banking or fraud in transactions.

3.5) ***Poor law Enforcing Bodies*****:** Due to lack in cyber laws of many countries, many criminals get away without being punished.

Case 3: Financial Crimes

Wipro Spectramind lost the telemarketing contract from Capital one due to an organized crime. The telemarketing executives offered fake discounts, free gifts to the Americans in order to boost the sales of the Capital one. The internal audit revealed the fact and surprisingly it was also noted that the superiors of these telemarketers were also involved in the whole scenario.

3.6) ***Cyber Crimes committed for publicity or recognition*****:** Generally committed by youngsters where they just want to be noticed without hurting someone's sentiments.

4 CYBER CRIME INVESTIGATIONS

Research has shown that no law can be fully brought into function to eradicate cyber crimes. The year 2012 experienced 61 % increase in cyber crimes totalling to 2, 876 with Maharashtra recording the most number of cases. A total of 176, 276, 356, 422 and 601 cases were registered under cyber crime related sections of the Indian Penal
Code (IPC) during 2008, 2009, 2010, 2011 and 2012. The past year illustrated how quickly the threat landscape continues to evolve, with risk to organisations continues to be amplified and it's now expanding across diverse mobile platforms. The Web sense Security Lab reinforced that traditional security measures are no longer effective in eradicating cyber attacks. The security providers need to evolve towards more practical defences. Here some Case studies have been included to elaborate on the threats and methods of defending against cyber attacks:

Case 1: Phishing Case Study

One Doctor from Gujarat had registered a crime stating that some persons (“perpetrators”) have perpetrated certain acts through misleading emails ostensibly emanating from ICICI Bank’s email ID. Such acts have been perpetrated with intent to defraud the Customers. The investigation was carried out with the help of the mail received by the customer, bank account IP details & domain IP information, the place of offence at was searched for evidence.

Case 2: On line credit Cheating and Forgery Scam

In one of the noted cases of 2003, Amit Tiwari, a 21yr old engineering student had many names, bank accounts and clients with an ingenious plan to defraud a Mumbai based credit card processing company, CC Avenue of nearly Rs. 900, 000.

5 EVOLUTION OF CYBER CRIMES:

5.1 As noted from the above three cases, predefined safety from cyber crimes to safeguard the network of agencies are important. The cyber criminals detect security holes which career criminals or even cyber-terrorist could use to attack them in future. Safeguarding and monitoring wireless access points, network access points, and network-attached devices by securing interfaces between agency-controlled and non-agency controlled or public networks, Standardizing authentication mechanisms in place for both users and equipment, Controlling users' access to information resources.

5.2 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.

5.3 Networks that serve different agencies or departments should be segregated, and access to those segmented networks should be established as appropriate through the use of VLANs, routers, firewalls, etc.

5.4 Access badges should 1 be programmed to allow entry only into assigned places of duty like after the Wipro Spectramind case, thorough security check of employees takes place and Mobile phone use is prohibited and technology is used to monitor data records.

5.5 Users' activities on systems should be monitored.

5.6 To prevent unauthorized access of information all hosts that are potential targets of DoS(Denial of Service) should be secured.

5.7 Authentic programs should be installed with Trojan scan Programs.

Cyber crime is one of the fastest-growing and most potentially damaging hazards that come with living in the digital age. The Bureau of Justice Statistics has identified three categories of cyber crimes as most prevalent:

Cyber attacks target computer systems. They include computer viruses such as worms and Trojan horses, as well as denial of service attacks and electronic vandalism or sabotage.

- Cyber theft involves crimes in which a computer is used to steal money or information. It includes embezzlement, fraud, theft of intellectual property and theft of personal or financial data.

- Other computer security threats include spyware, adware, hacking, phishing, spoofing, pinging and port scanning. One thing to note: an attempt is a crime regardless of whether the breach is successful.

Incidents of cyber crime can also involve preying on individuals and groups through cyber abuse and online bullying. Cyber crime manages to reach nearly every group of people and all types of organizations through one mechanism or another. Research indicates one in six adults have experienced some incident of electronic threat or crime.

.

The Cost of Cyber Crime In terms of dollars lost to companies and individuals, as well as what it costs the Federal Bureau of Investigation and other law enforcement agencies to fight it, cyber crime costs billions of dollars. According to the Infosec Institute, cyber crime costs the United States $100 billion a year and $300 billion globally. As more and more business activity and personal interactions move to online platforms, this is a number that will likely continue its upward trend.

Protecting Yourself from Cyber Crime What can be done to fight cyber crime? The good news is that you have several ways to protect yourself, your family and your electronic devices from the threat of shadowy cyber activity.

Use smart passwords. The simpler your passwords are, the more they put you at risk. Make sure they're at least eight characters long and contain a variety of letters, numbers and symbols. Keep them in a secure place, and don't share them with anyone you don't completely trust. Use a phrase as a memory aid to help you create and remember a more complex password structure.

- Be careful when visiting websites. Unfamiliar websites or objectionable content sites are well-known breeding grounds for cyber attacks. Consider avoiding those where you run the risk of being exposed to potential cyber criminals.

- Consider installing reliable anti-virus, anti-spyware and Internet filtering programs on your devices. These threefold protective systems help ensure that you don't accidentally encounter viruses or hacking threats. After you've downloaded one of these programs, be sure to install any updates as soon as they become available or consider turning on an auto-update feature if available. One of the most common ways cyber criminals gain access to electronic devices is by hacking outdated systems.

- Keep your computer's operating system up-to-date. According to the FBI, this can go a long way toward protecting your device. Computer operating systems are updated periodically to stay in tune with technological advancements and to fix security holes. Install updates to ensure your computer has the latest protection, as old versions may become unsupported by their authors over time.

- Download carefully. Dangerous e-mail attachments can circumvent even the most vigilant anti-virus software. Beware of opening anything from someone you don't know. You should even be wary of forwarded attachments from people you do know. E-mail attachments can contain malicious code intended to harm your computer or electronic devices.

- Shut down your computer when it's not in use. It's tempting to leave it on at all times so you have quick access when you need it, but the more time your computer stays on, the more time each day it's vulnerable. Powering your computer off on a regular basis effectively eliminates a hacker's connection, and allows auto-updating to occur as needed when you reconnect.

5.8 PRECAUTIONS TO PREVENT CYBER CRIME:

Nobody's data is completely safe. But everybody's computers can still be protected against would-be hackers as follows:

1. Firewalls: These are the gatekeepers to a network from the outside. Firewall should be installed at every point where the computer system comes in contact with other networks, including the Internet a separate local area network at customer's site or telephone company switch.

2. Password protection: At minimum, each item they logon, all PC users should be required to type-in password that only they and network administrator know. PC users should avoid picking words, phrases or numbers that anyone can guess easily, such as birth dates, a child's name or initials. Instead they should use cryptic phrases or numbers that combine uppercase and lowercase. Letters such as the "The Moon Also Rises". In addition the system should require all users to change passwords every month or so and should lockout prospective users if they fail to enter the correct password three times in a row.

3. Viruses: Viruses generally infect local area networks through workstations. So anti-virus software that works only on the server isn't enough to prevent infection. You cannot get a virus or any system-damaging software by reading e-mail. Viruses and other system-destroying bugs can only exist in files, and e-mail is not a system file. Viruses cannot exist there. Viruses are almost always specific of the operating system involved. Meaning, viruses created to infect DOS application can do no damage to MAC systems, and vice versa. The only exception to this is the Microsoft Word "macro virus" which infects documents instead of the program.

4. Encryption: Even if intruders manage to break through a firewall, the data on a network can be made safe if it is encrypted. Many software packages and network programs – Microsoft Windows NT, Novel NetWare, and lotus notes among others- offer and – on encryption schemes that encode all the data sent on the network. In addition, companies can buy stand alone encryption packages to work with individual applications. Almost every encryption package is based on an approach known as public-private key

Scrambled data is encoded using a secret key unique to that transmission. Receiver's use a combination of the sender's public key and their own private encryption key to unlock the secret code for that message decipher it.

5. Never send your credit card number to any site which is not secured.

6. Uninstall unnecessary software

5.9 Computer Virus Protection: Computer viruses are computer programs that, when opened, put copies of themselves into other computers' hard drives without the users' consent. Creating a computer virus and disseminating it is a cyber crime. The virus may steal disk space, access personal information, run data on the computer or send information out to the other computer user's personal contacts., such as diskettes or CDROMs, validating the source of software before installing it all CDs or other media brought from home or any other outside

6 CONCLUSIONS

It has been deducted from this present study that with increasing rate of cyber crimes more detection techniques along with educating the users on being safe online needs to be established with complete guidance to know about the pros and cons of the web before entering it. There is no doubt that the Internet offers criminals several opportunities. Information is the best form of protection. Concrete measures must be found in order to track electronics evidence and preserve them so that systems are better protected from cyber intrusions. Besides, new cyber laws and policies must be developed by to tackle the various families of cyber crime. Even the companies need to take appropriate measures to investigate and prevent their data.

7) REFERENCES

[1] Dacey, Raymond & Gallant, Kenneth S. (1997) "Crime control and harassment
of the innocent, " Journal of Criminal Justice, Elsevier, vol. 25(4), pages 325-
334.

[2] H. Choi, H. Lee, H. Lee, and H. Kim (2007) "Botnet Detection by Monitoring
Group Activities in DNS Traffic, " in Proc. 7th IEEE International Conference on Computer and Information Technology (CIT2007)

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

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

[5] Michael Massourakis & Farahmand Rezvani & Tadashi Yamada (1984) "Occupation, Race, Unemployment and Crime .715-720.

In a Dynamic System, " NBER Working Papers 1256, National Bureau of Economic Research, Inc.

[6] 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.

[7] Ying-Chieh Chen, Patrick S. Chen, Jing-Jang Hwang, Larry Korba, Ronggong Song, George Yee, (2005) "An analysis of onlinegami