International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN : 2456-3307

Cyber Crime - The Biggest Problem of World Today

Neha Bansal, Simran Saini, Charanjeet Kaur Raina

Department of Computer Science Engineering Adesh Institute of Technology,Gharuan, Chandigarh campus, Punjab, India

ABSTRACT

Hackers are the smartest people on the earth. They always try to steal and reveal someone's personal information. Sometimes the reason behind hacking is not to learn something but to take revenge by reveal/blackmailing to reveal their personal information to the world or sometimes it may be their greed. Thus sometimes it leads to suicide cases. Hackers are always one step more than cyber forensics investigators. It is a rat and cat race.

Keywords : Hackers, Hacking, Cyber-Crime, Denial-Of-Service, DDOS Attacks, APDOS Attacks, BlackBerry Messenger, IVR, Cell Site Analysis

I. INTRODUCTION

What is Cyber Crime? Cyber-crime generally involves computer and network for stealing the personal information without his/her permission and reveals that information to world and thus harms them. It is also defined as "Offences that are committed against individuals or groups of individuals with a criminal motive to harm their reputation or cause physical or mental harm, or loss, to the victim directly or indirectly, by using modern telecommunication networks system such as Internet and mobile phones (Bluetooth/SMS/MMS)". Cyber-crime may threat the national's security as well as the financial health.

The Computer as a Target : Using a computer to attack other computer e.g. Hacking, Virus/Worm attacks, DOS attack etc.

The Computer as a Weapon: Using a computer to commit real world crimes e.g. Cyber Terrorism, IPR violation, Credit card frauds, EFT frauds, pornography, etc.

Cyber-crime is also called 5^{th} generation war.

Fifth generation war generally the cyber war including cyber-crime generally don't includes any short fire even then they can achieve their aims.

MOTIVES BEHIND CYBER CRIME:

- ✓ Greed
- ✓ Power
- ✓ Publicity
- ✓ Revenge
- ✓ Adventure
- ✓ Desire to access forbidden information
- ✓ Destructive mind-set

II. METHODS AND MATERIAL

1. CHALLENGES FOR CYBER SECURITY:

- **DOS Attacks:** A denial-of-service (DOS) attack is a security event that occurs when an attacker takes action that prevents legitimate users from accessing targeted computer systems, devices or other network resources. Generally there is a degradation of network while opening the files which are generally stored on network or while opening any site on browser.
- **DDOS Attacks:** It is a distributed denial-of-services (DDOS) attacks. DDOS is a type of DOS attack whose aim is to disrupt the actual/normal function of particular website The Victims of a DDOS attack consist of both the end target system

and all systems maliciously used and controlled by the hacker. DDOS attacks are often global attacks, distributed via botnets and goal is to make the website unavailable to its regular visitors.

- **APDOS Attacks:** Advanced persistence denial-of-service (APDOS) attacks does a clear and emerging threat need specialised Monitoring and Incident Response services and the defensive capabilities of specialised DDOS mitigation service providers. It generally attacks simultaneous Multi-threaded ISO layer.

How Hackers hacks someone account? Generally **Phishers** send an email that appears to be come from any bank and credit company. This e-mail contains a link to fraud website/webpage including company's logos and content. When click on the link it is requesting for your personal information including your bank details and contact number, ATM's pin or credit card's number. After filling that information OTP was send to your mobile. After that they block your number from that transaction and then transfer money. Actually this would happen with people.

WATER HOLING

Water holing is the attacking strategy generally used by hackers in which they attack the particular group/industries/organization/region. In this attacker/hackers observe which website is generally used by group and thus they infect one of them with malicious virus/malware. Thus some of members of target group get infected and thus hackers can gain access to secure system.

BAITING

Baiting is like a real world Trojan horse which relies on greed/curiosity of victim. The attacker creates a physical disk with corporative logos and then leaves that disk on the floor of elevator or in lobby of Target Company. An unknown employee find it and insert it into the computer to satisfy the curiosity but good one may find it then return to company. By just inserting the disk in computer install the malware and giving the access to victim's PC, the target company's internal computer network.

PHONE PHISHING (VISHING)

This generally uses a scamp **Interactive Voice Response (IVR)** system to recreate the legitimate the sound copy of bank or other institute's IVR system. The victim is calling into bank usually toll free number provided in order to 'verify' number. This vishing system generally reject login continued and the victim enters the pin number multiple times, generally disclose the several password.

BBM (BlackBerry Messenger)

BBM is an internet based messaging app in blackberry smartphones generally supports extreme security in messaging through advanced encryption techniques. This extreme security is now risking for national security as encrypted messages are not accessed even by RIM (Research in Motion) who released this blackberry in 2001 (A Canadian company). Criminals use this BBM for communications among them as can't even decrypt by even company. So such mobiles are banned in some country as not easy to decrypt the message that creates a lot of problems while solving the case related to cyber-crime.

CYBER FORENSICS

Cyber forensics is the branch of digital forensics science for collecting, analysis, and reporting on digital data such that it is legally allowable. It generally investigates and analysis for gathering and preserving evidences from particular device in such a way that it is suitable for presenting in court. Sometimes for retrieving the Data from server (situated in USA) legally takes a lot of times even for cyber experts.

Bureau of Police Research and Development was set up on 28 August 1970 for modernising the police forces by proving training to them time to time by introducing new technologies.
BPRD generally have four divisions: Research, Training, Development, and correctional Administration.

RESEARCH DIVISION: Generally analysis and study the crime, prevention of crime-preventives measures, improvements in methods of investigation, statistical analysis of trends of crime.

TRAINING DIVISION: To review time to time new scientific technologies and give training to police officers,

DEVELOPMENT DIVISION: Review the performance of equipment used by police force in India, develop new equipment for Riot Control Equipment or for Police Transport, work related to Police research & Development Advisory Council and its Committees, not on police research

CORRECTIONAL ADMINISTRATION DIVISION: Analysis and study of Prison statistics also setup an Advisory Committee for guiding the work related to Correctional Administration.

CELL SITE ANALYSIS (CSA)

Cell Site Analysis is a process which identifies the location and movement of a mobile phone over a period of time. This process cross-references of historic call records which generally includes voice, SMS and multimedia messages with readings from the cell site masts that transmit and receive mobile communication signals. CSA allows forensics investigators to identify particular locations in which single or multiple mobiles phones are used. It also track the changes the physical location and identify line of use or non-use. It also identifies the contact between the different mobile devices content, time and location based.

INFORMATION OBTAIN FROM THE DEVICE

- ✓ Phonebook
- ✓ Call History and details(To/From)
- ✓ Call durations
- ✓ Text message with identifiers(send to, and originating) sent, received, deleted messages
- ✓ Multimedia Text Messages with Identifiers
- ✓ Photos and Videos(also stored on external flesh)
- ✓ Sound Files(also stored on external flesh)
- ✓ Network Information, GPS Location
- ✓ Phone IMEI serial no.

III. RESULTS AND DISCUSSION

CASE STUDY

A lady got hit by a ransomware (a type of malicious software designed to block access of computer system until money is paid) attack. 5,726 files got locked by CryptoWall (an encryption malware). It is very powerful that technically it is impossible to break open. She contacted the attacker via the ransomware's communication feature and told her that she can either pay to get her files back or lose them forever. Despite backing up her files, she decided that losing of photos, documents and other files was too much, and so she decided to pay him. The price for unlocking her files was $500 in the first week and $1000 in the second one, after which the files would be deleted. Payment was to be done in Bitcoin (a digital currency created and held electrically. No one control it), an obscure and unfamiliar process which she had to learn on the fly. Because of a major snowstorm the banks are closed, she couldn't pay the ransom in the first week, and ended up with plea to attacker for not increasing the price to 1,000$. He accepted and gave her the key to unlock her files.

NOTHING IS SECURE

Can u think that if we buy a 2 GB pen drive, it costs Rs. 200 but Google give us 15 GB space while making Gmail account at free of cost? Also if we want to receive our personal data from either Google or from any other account then it may take 1 year (approx.) legally as there are no servers of any Google/Facebook/Whatsup in India. They generally steal our data and store in USA (where server of these are made).

Even India is a country where all the foreign companies sell their products. India is a country of selling not of making. We have no our own operating system, software, firewalls etc.

When our computer is off we are not doing anything; still it can't be hacked; even if you leave it connected to the internet and to power. There is a feature in the network adapter that (when enabled) allows a computer to be remotely turned on and booted.

Sometimes our own ignorance also gives chance to hacker for hacking. Why they break wall if we itself enter them in our computer. Like a mail you received from well-known legitimate company and ask for filling your personal information when click on link. Sometimes that link contain some malicious virus just by clicking on that link our device is hacked. So be careful while clicking on any link.

We don't even want to show our personal pictures to our friends. There is a password in our mobile phone, especially to our gallery. But when we synchronised our all the mobile data to our Google account in android or icloud in IOS, we itself give permission for our personal pictures to accessed by USA. After that we think we are secured!!!!

NOTHING IS SECURED….

EVERYTHING IS POSSIBLE IN TODAYS WORLD.

So don't be stupid, be creative in cyber world, Use knowledge to save ourselves as well as our country, respecting our Country's Cyber Law

IV.CONCLUSION

- ✓ Cyber Crime statistics show businesses/gender meets prominent targets.
- ✓ Cyber Security and forensics is an important issue.
- ✓ Learn something Need of training Polices/prosecution/judiciary time to time so as to introduce about latest technology.
- ✓ Need of expeditious traits
- ✓ Collaboration between Law Enforcement /Academician/Cyber techno/Cyber Dome of Kerala NASSCOM labs/treat of Excellences in Bengaluru is the best practices.
- ✓ BPRD (Bureau of Police Research and Development) playing a very vital role in bringing all together.
- ✓ Most of the cyber-crimes are solved if India has its own servers and its application as it take less time as compared to the time for access the data from server situated at USA.

Conventional + Cyber Investigsation = Cyber Security

V. REFERENCES

[1]. Bureau of Police Research and Development. Retrieved from

[2]. https://en.m.wikipedia.org/wiki/Bureau_of_Police_Research_and_Development

[3]. Connecting police for a safer world. Retrieved from http://searchsecurity.techtarget.com/definition/computer-forensics

[4]. Cyber Law Cases in India and World. Retrieved from http://www.cyberlawsindia.net/cases.html

[5]. Cybercrime. Retrieved from https://en.m.wikipedia.org/wiki/Cybercrime

[6]. Here's How Hackers Stole $80 Million from Bangladesh Bank. (2016, March 14). Retrieved from http://thehackernews.com/2016/03/bank-hacking-malware.html

[7]. Rouse Margaret. Cybersecurity. Retrieved from http://whatis.techtarget.com/definition/cybersecurity

[8]. Rouse Margaret . denial-of-service attack. Retrieved from http://searchsecurity.techtarget.com/definition/denial-of-service

[9]. Top 5 Popular Cybercrime: How can you easily prevent them. Retrieved from http://www.enigmasoftware.com/top-5-popular-cybercrimes-how-easily-prevent-them/