RESEARCH PAPER
Computer Science
Volume : 3 | Issue : 5 | May 2013 | ISSN - 2249-555X

Cyber Crime & its Categories

KEYWORDS

Kejal Chintan Vadza

Asst. Prof. at Sutex Bank College of Computer Applications & Science,Amroli, Surat,Gujarat - 395009

ABSTRACT *Cyber Crime research paper includes basic introduction about internet related crimes and its various categories.*

Introduction to Cyber Crimes:
Cyber Crime can be defined as unlawful acts committed by using the computer as a tool or as a target or as both. Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery (copy), defamation (insult) and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut (range) of new age crimes that are addressed by the Information Technology Act, 2000 (introduced on 17th Oct 2000)

5.1) Cyber crime can be **categorized** mainly in two ways:

- Using the Computer as a Target:-using a computer to attack other computers. e.g. Hacking, Virus/Worm attacks, DOS attack etc.
- Using the computer as a weapon:-using a computer to commit real world crimes. e.g. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc.

Moreover we further categorized as follows:

1. Unauthorized Access:

Access means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network. Unauthorized access would therefore mean any kind of access without the permission of either the rightful owner or the person in charge of a computer, computer system or computer network.

2. Hacking & Cracking:

Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. Crackers may steal or modify data or insert viruses or worms which damage the system. By hacking web server taking control on another person's website called as web hijacking

3. Cyber Fraud/Online Fraud:

The net is a boon for people to conduct business effectively, very quickly. Net is also an open invitation to fraudsters and online frauds are becoming increasingly out of control.

1. Spoof websites and email security alerts Fraudsters create authentic looking websites that are actually nothing but a spoof. The purpose of these websites is to make the user enter personal information. This information is then used to access business and bank accounts. If you ever get an email containing an embedded link, and a request for you to enter secret details, treat it as suspicious. Do not input any sensitive information that might help provide access to your accounts, even if the page appears legitimate. No reputable company ever sends emails of this type.

2. Virus hoax emails

It is a sad fact of life that there are those who enjoy exploiting the concerns of others. Many emailed warnings about viruses are hoaxes, designed purely to cause concern and disrupt businesses.

These warnings may be genuine, so don't take them lightly, but always check the story out by visiting an antivirus site such as McAfee, Sophos or Symantec before taking any action, including forwarding them to friends and colleagues.

3. Lottery Frauds

These are letters or emails, which inform the recipient that he/ she has won a prize in a lottery. To get the money, the recipient has to reply. After which another mail is received asking for bank details so that the money can be directly transferred. The email also asks for a processing fee/ handling fee. Of course, the money is never transferred in this case, the processing fee is swindled and the banking details are used for other frauds and scams.

4. Spoofing

Spoofing means illegal intrusion, posing as a genuine user. A hacker logs-in to a computer illegally, using a different identity than his own. He is able to do this by having previously obtained actual password. He creates a new identity by fooling the computer into thinking he is the genuine system operator. The hacker then takes control of the system. He can commit innumerable number of frauds using this false identity.

In short spoofing refers to thing that appears to have been originated from one source when it was actually sent from another source

5. Credit Card Fraud

Online Transaction has become a normal thing in day today life. Knowingly or unknowingly passing credit card information over internet can land you in trouble. If electronic transactions are not secured the credit card numbers can be stolen by the hackers who can misuse this card by impersonating the credit card owner.

4. Cyber Theft:

Stealing of financial and/or personal information through the use of computers for making its fraudulent or other illegal use.

Identity Theft:-
Identity theft occurs when someone appropriates another's personal information without their knowledge to commit theft or fraud. Identity theft is a vehicle for perpetrating other types of fraud schemes.

Theft of Internet Hours:-
Unauthorized use of Internet hours paid for by another person.

Theft of computer system (Hardware):-
This type of offence involves the theft of a computer, some part(s) of a computer or a peripheral attached to the computer.

5. **Cyber Terrorism:**
   Targeted attacks on military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks are the most likely targets. Others like police, medical, fire and rescue systems etc.
   Cyber terrorism is an attractive option for modern terrorists for several reasons.

1. It is cheaper than traditional terrorist methods.
2. Cyberterrorism is more anonymous than traditional terrorist methods.
3. The variety and number of targets are enormous.
4. Cyberterrorism can be conducted remotely, a feature that isespecially appealing to terrorists.
5. Cyberterrorism has the potential to affect directly a larger number of people.
6. Flowing of Virus, Trojan horse, Worm & Logical Bombs:

The program that act like something useful but do the things that are quiet damping. The programs of this kind are called as Trojans. Trojans come in two parts, a Client part and a Server part. When the victim (unknowingly) runs the server on its machine, the attacker will then use the Client to connect to the Server and start using the trojan.TCP/IP protocol is the usual protocol type used for communications, but some functions of the trojans use the UDP protocol as well.

A program that has capability to infect other programs and make copies of itself and spread into other programs is called virus. Viruses can often spread without any readily visible symptoms. A virus can start on event-driven effects (for example, triggered after a specific number of executions), time-driven effects (triggered on a specific date, such as Friday the 13th) or can occur at random. Action of a virus can be display a message to prompt an action which may set of the virus,Erase files,Scramble data on a hard disk,Cause erratic screen behavior,Halt the PC…..etc

Programs that multiply like viruses but spread from computer to computer are called as worms. **For ex. Anna Kournikova worm(feb-2001)The first computer virus ever to be see was called BRAIN and it appeared in 1986. Some famous viruse are…** Jerusalem (1987), Dark Avenger (1989), Michelangelo (1991), Concept (1995), Melissa , CIH (1999), The Love Letter (2000), CodeRed, Nimda (2001), SirCam-Nimda…Etc.

Logical bombs are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. E.g. even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the **Chernobyl virus**).

7. **Cyber Pornography:**
   Pornography' is "describing or showing sexual acts in order to cause sexual excitement through books, films, etc." This includes pornographic websites; pornographic material produced using computers and use of internet to download and transmit pornographic videos, pictures, photos, writings etc. There are more than 420 million individual pornographic webpages today. Child pornography is a very unfortunate reality of the Internet. The Internet is being highly used by its abusers to reach and abuse children sexually, worldwide.

Pedophiles use a false identity to trap the children/teenagers

8. **Defamation:**
   Defamation can be understood as the intentional infringement of another person's right to his good name. Defamation can be understood as tarnishing the image, respect or dignity of any person in front of right thinking members of the society.

Cyber Defamation occurs when defamation takes place with the help of computers and / or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends A matter defaming a person is sent to the said person directly is not defamation however if the said mail is sent through CC or BCC to third parties and if the contents tarnish (blemish/dull) the image of the recipient it is defamation. Publication of defamatory articles and matter on a website are defamation. **Cyber defamation is also called as Cyber smearing.**

9. **Cyber Stalking:**
   Cyber Stalking can be defined as the repeated acts harassment or threatening behavior of the cyber criminal towards the victim by using Internet services. (**OR** Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc.)

Stalking in General terms can be referred to as the repeated acts of harassment targeting the victim such as…

1. Following the victim
2. Making harassing phone calls
3. Killing the victims pet
4. Vandalizing victims property
5. Leaving written messages or objects

Stalking may be followed by serious violent acts such as physical harm to the victim and the same has to be treated and viewed seriously. It all depends on the course of conduct of the stalker. Both kinds of stalkers – online and offline - have desire to control the victim's life.

Cyber-stalking refers to the use of the Internet, e-mail, or other electronic communications device to stalk another person. It is a relatively new form of harassment, unfortunately, rising to alarming levels especially in big cities like Mumbai.

10. E-mail & IRC related crimes:
1. Email spoofing
Email spoofing refers to email that appears to have been originated from one source when it was actually sent from another source. Please Read

2. Email Spamming:
Email "spamming" refers to sending email to thousands and thousands of users - similar to a chain letter is called email spamming. Email spam targets individual users with direct mail messages. Email spam lists are often created by scanning Usenet postings, stealing Internet mailing lists, or searching the Web for addresses. Email spam, also known as junk email or unsolicited bulk email (UBE), is a subset of electronic spam .

3. Email bombing
E-mail "bombing" is characterized by abusers repeatedly sending an identical email message to a particular address.

5. Sending threatening emails
Email is a useful tool for technology savvy criminals thanks to the relative anonymity offered by it. It becomes fairly easy for anyone with even a basic knowledge of computers to be-

come a blackmailer by threatening someone via e-mail.

6. Defamatory emails
Cyber-defamation or even cyber-slander as it is called can prove to be very harmful and even fatal to the people who have been made its victims. **OR**

Defamation is defined as communication to third parties of false statements about a person that injure the reputation of or deter others from associating with that person.A communication is not defamatory unless it is published to someone other than the target.

7. Email frauds
Email Fraud is the intentional deception made for personal gain or to damage another individual through email. Almost as soon as email became widely used, it began to be used as a means to defraud people. Email fraud can take the form of a "con game" or **scam.**

8. IRC related
Internet Relay Chat (IRC) is a protocol for real-time Internet text messaging (chat) or synchronous conferencing. It is mainly designed for group communication in discussion forums, called **channels,** but also allows one-to-one communication via private message as well as chat and data transfer, including file sharing. "Chat room" is another name for an **Internet Relay Chat (IRC)** channel

Internet Relay Chat (IRC) Crime:
- Criminals use it for meeting coconspirators.
- Hackers use it for discussing their exploits / sharing the techniques
- Pedophiles use chat rooms to allure small children

Three main ways to attack IRC are: attacks, clone attacks, and flood attacks.

11. Spamming:
Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. Most spam is commercial advertising. For ex. get-rich-quick schemes.
There are two main types of spam, and they have different effects on Internet users. 1)Cancellable Usenet / Usenet spam & 2) Email-spam

1. Cancellable Usenet spam is a single message sent to 20 or more Usenet newsgroups.
2. Email "spamming" refers to sending email to thousands and thousands of users - similar to a chain letter. Email spam, also known as junk email or unsolicited bulk email (UBE), is a subset of electronic spam . One subset of UBE is UCE (unsolicited commercial email). Spammers collect email addresses from chatrooms, websites, customer lists, newsgroups, and viruses which harvest users' address books, and are sold to other spammers. They also use a practice known as "email appending" or "epending" in which they use known information about their target (such as a postal address) to search for the target's email address.

12. Denial of Service attacks:-
Flooding a computer resource with more requests than it can handle. This causes the resource to crash thereby denying access of service to authorized users.

Examples include
attempts to "flood" a network, thereby preventing legitimate network traffic
attempts to disrupt connections between two machines, thereby preventing access to a service
attempts to prevent a particular individual from accessing a service
attempts to disrupt service to a specific system or person.

13. Forgery:
Counterfeit currency notes, postage and revenue stamps, mark sheets etc can be forged using sophisticated computers, printers and scanners.Also impersonate another person is considered forgery.

14. IPR Violations:
These include software piracy, copyright infringement, trademarks violations, theft of computer source code, patent violations. etc.Cyber Squatting- Domain names are also trademarks and protected by ICANN's domain dispute resolution policy and also under trademark laws. Cyber Squatters registers domain name identical to popular service provider's domain so as to attract their users and get benefit from it.

15. E-commerce/ Investment Frauds:-
Sales and Investment frauds. An offering that uses false or fraudulent claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities. Merchandise or services that were purchased or contracted by individuals online are never delivered. The fraud attributable to the misrepresentation of a product advertised for sale through an internet auction site or the non-delivery of products purchased through an Internet auction site. Investors are enticed to invest in this fraudulent scheme by the promises of abnormally high profits.

16. Sale of illegal articles:
This would include trade of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication.Research shows that number of people employed in this criminal area. Daily peoples receiving so many emails with offer of banned or illegal products for sale.

17. Online gambling:
There are millions of websites hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering.

18. Data diddling:
Data diddling involves changing data prior or during input into a computer.
In other words, information is changed from the way it should be entered by a person typing. in the data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file.
It also include automatic changing the financial information for some time before processing and then restoring original information.

19. Physically damaging a computer system:
Physically damaging a computer or its peripherals either by shock, fire or excess electric Supply etc.

20. Breach of Privacy and Confidentiality:

Privacy
Privacy refers to the right of an individual/s to determine when, how and to what extent his or her personal data will be shared with others.

Breach of privacy means unauthorized use or distribution or disclosure of personal information like medical records, sexual preferences, financial status etc.

Confidentiality
It means non disclosure of information to unauthorized or unwanted persons.

In addition to Personal information some other type of information which useful for business and leakage of such information to other persons may cause damage to business or person, such information should be protected.

Generally for protecting secrecy of such information, parties while sharing information forms an agreement about he procedure of handling of information and to not to disclose such information to third parties or use it in such a way that it will be disclosed to third parties.

Many times party or their employees leak such valuable information for monitory gains and causes breach of contract of confidentiality.

Special techniques such as Social Engineering are commonly used to obtain confidential information.

REFERENCE

Ref: (book cyber crime in india – Dr. M. Dasgupta.) | http://lawincyber.wordpress.com/2010/08/04/3333/ | http://vinlawyer.com/cybercrime.html | http://www.cyberlawsindia.net/ |