Cyber Crime and Security

Darshit Shah, Lokesh V.Soni ,Dharmit Tailor,Pratyush Shukla

Department of Computer Engineering, Thakur Polytechnic,Mumbai, India

---***---

Abstract: Electronic document gives the overview of Cyber Crime. Cyber crime is also known as computer crime. Such as phishing, credit card frauds, bank robbery, illegal downloading, child pornography, kidnapping children via chat rooms, scams, cyber terrorism, creation and spreading of viruses, Spam etc. It uses a computer as an instrument for the illegal things, such as committing fraud and intellectual property, hacking accounts. Because of wide use of internet, the importance of cybercrime has grown as the computer has become central to commerce, entertainment and government. Mostly the cybercrime is an attack on data or information about individuals, corporations or government. Now days, in the digital world any person's virtual identities are important elements of day to day life means the information about individuals can be used in multiple computer databases owned by governments and corporations.

I. INTRODUCTION TO CYBER CRIME:

Cyber crime is a basic term that refers to all criminal activities done using the medium of computers, the Internet and the worldwide web. Cybercrime ranges across a variety of activities. At one end are crimes that involve fundamental violation of personal or corporate privacy, such as physical attacks on the integrity Depositories and the use of illegally within corporations or government organizations deliberately altering data for either profit or political objectives.

Figure 1. Cyber crime.

The criminal hides it in the relative anonymity which is provided by the internet. There are other crimes that involve attempts to disrupt the actual workings of the internet. It also involves individuals obtained digital information to blackmail a firm or individuals. Also at this end of the spectrum is the growing crime of identity theft. There are transaction-based crime like: fraud, pornography, digital piracy, money laundering and counterfeiting.

Figure 2. Cyber crime.

II. TYPES OF CYBER CRIME

a) Financial: This crime disrupts businesses ability to conduct 'e-commerce'.

b) Piracy: this is related to the act of copying copyrighted material. The personal computer and the internet both offer new way for an 'old' crime. Online theft is known as any type of piracy or private data that involves the use of the internet to market or distribute creative works protected by copyright.

c) Hacking: this crime is related to the act of gaining illegal access to a computer system or network and sometime making unauthorized use of such access. Also, it is the act by which other forms of cyber-crime like fraud, terrorism, etc. are committed.

d) Cyber terrorism: The main outcome of act of hacking is designed to cause terror. E-terrorism is the result of hacking, which will cause violence against persons or property, or at least cause enough harm to generate fear like other conventional terrorism.

e) Online pornography: There are laws against possessing or distributing child pornography. Distributing pornography of any form to a minor is illegal. The Internet is merely a new medium for this 'old' crime, but how best to regulate this global medium of communication across international boundaries and age groups has sparked a great deal of controversy and debate.

f) Sabotage: It is another type of the hacking involves the hijacking of a government or corporation web site. It means a purposeful destruction of property or slowing down of work with the intension of damaging a business or economic system or weakening a government or nation in a time of national emergency.

III. HACKING

Hacking: Hacking is one of the most well-known types of the computer crime. A hacker is someone who find out and exploits the weaknesses of a computer system or network. It refers to the unauthorized access of another's computer system. These intrusions are often conducted in order to launch malicious program known as virus, worms and Trojan horses that can shut down or destroy an entire computer network. Hacking is also carried out as a way to take credit card number, internet password, and other personal information. By accessing commercial databases, hackers are able to steal these types of item from millions of internet users all at once. Basically there are five type of hacker.

Figure 3. Hacking.

a) White Hat: This type of hacker is someone who has non-malicious whenever he breaks into security system. A white hat that does vulnerability assessments and penetration tests is also known as an ethical hacker.

b) Black Hat : This type of hacker is also known as cracker and he a malicious purpose whenever he goes about breaking into computer security systems with the use of the technology such as a network, telecommunication system, or computer and without authorization. His malicious purpose can range from all sorts cybercrimes such as piracy, identity theft, credit card fraud, damage, and so forth. He may or may not utilize questionable tactic such as deploying worms and malicious sites to meet his ends.

c) Grey Hat: A grey hat hacker is the combination of the black hat and the white hat. this is the kind of hacker that is not a penetration tester but will go ahead and surf the internet for vulnerable system he could exploit. Like a white hat, he will inform the administrator of the website of the vulnerabilities he found after hacking through the site. Like a black hat and unlike a pen tester, he will hack any site freely and without any prompting or authorization from owners what so ever. He will even offer to repair the vulnerable site he exposed in the first place for a small fee.

d) Elite Hacker: As with any society, better than average people are rewarded for their talent and treated as special. this social status among the hacker underground, the elite are the hackers among hackers in this subculture of sorts. They are masters of deception that have a solid reputation among their peers as a cream of the hacker crop.

e) Script kiddie: A script kiddie is basically an part-time or non-expert hacker, who break into peoples computer systems not through his knowledge in IIT security and the ins and outs of a given website.

IV. CRACKING

Figure 4. Cracking.

Cracking: In the cyber world , a cracker is someone who breaks into a computer system or network without authorization and with the intention of doing damage. Cracking is used to describe a malicious hacker. Cracking can be done for the profit, maliciously, for some harm to organization or to a individuals. Cracking activity is harmful, costly and unethical. Cracker get into all kind of mischief like he may destroy files, steal personal data like credit card numbers or client data, infect the system with a virus, or others things that can cause harm to the system. Cracking can be done for profit, maliciously, for some harm to organization or to a individuals. Cracking activity is harmful, costly and unethical.

V. CYBER CRIME INVESTIGATION

Cyber Crime Investigation: Cyber crime investigations seek to determine the nature and collect evidence to lead to a conviction. An investigation is used to stop a crime in progress, report a past crime or to protect an individuals or organization from further harm. The way of investigation depends upon the type of crime for example in hacking, they need to uncover evidence where instruction occurred, and they will link it to a source. Investigation must carefully document all things through videotape, record keystrokes, and take other measures to track their activities.

Figure 5. Cyber crime investigation

Who is the cybercrime investigator: A computer crime cyber crime investigation is a person who work to solve crimes happening on the internet or other computer networks like work or school computer systems. A cybercrime investigator is responsible for identifying cases of computer related crimes like identifying the computer, server or network from where the criminal activity is generated. An investigation should known the laws and regulations related to computer and internet.

VI. CONCLUSION

The threat of computer crime is not as big as the authority claim. This means that the methods that they introducing to combat it represents an unwarranted attack on human rights and is not proportionate to the threat posed by cyber-criminals. The attempts to outlaw the possession of hacking software could harm people who trying to make the internet more secure as they will not be able to test their systems; therefore the legislation could do more harm than good.

REFERENCE

[1] www.google.com
[2] www.cybercellmumbai.gov.in/html/cyber-crimes
[3] http://www.cyberlawsindia.net/internet-crime.html
[4]http://study.com/academy/lesson/what-is-cyber-crime-definition-types-examples.html

[5] http://www.webopedia.com/TERM/C/cyber_crime.html