Cyber Crime- The review

Mahak Arora[1], Kamal Kumar Sharma[2], Sharad Chouhan[3]

[1]Student, M. Tech, E-Max group of Institutions, Ambala
[2]Professor, Dept. of ECE, E-Max group of Institutions, Ambala
[3]Assistant Professor, Deptt. of CS, E-Max group of Institutions, Ambala

Abstract: This document covers Cyber Crime. Computer crime, or Cybercrime, refers to any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Net crime is criminal exploitation of the Internet

Keywords: Denial-of-service, Malware, Phishing, Spam, Cyber Terrorism, Cyber Stalking.

I. INTRODUCTION

Dr. Debarati Halder and Dr. K. Jaishankar (2011) define Cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)". Such crimes may threaten a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding cracking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise.

An Australian nationwide survey conducted in 2006 found that two in three convicted cyber-criminals were between the ages of 15 and 26.

Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as cyber warfare. The international legal system is attempting to hold actors accountable for their actions through the International Criminal Court.

II. CYBER CRIME

Computer crime encompasses a broad range of activities. Generally, however, it may be divided into two categories: (1) crimes that target computers directly; (2) crimes facilitated by computer networks or devices, the primary target of which is independent of the computer network or device.

III. CLASSIFICATION

Crimes that primarily target computer networks or devices include:

- Computer viruses
- Denial-of-service attacks
- Malware (malicious code)

Crimes that use computer networks or devices to advance other ends include:

- Cyber stalking
- Fraud and identity theft
- Information warfare
- Phishing scams

Spam

The unsolicited sending of bulk email, for commercial purposes, is un-lawful in some jurisdictions. While anti-spam laws are relatively new, limits on unsolicited electronic communications have existed for some time. Another cyber crime that's kind of new is called phishing which is mostly used for emails. Phishing emails may contain links to other websites that are affected by malware. Sometimes it's even used when you are trying to do online banking and it says you're account number is incorrect. And then you're redirected to the page again and mostly there is a small change to your previous screen, but it's hard to recognize. If you fill in your personal information again then the phishers now know your bank account information.

1) Computer as tool

When the individual is the main target of Cybercrime, the computer can be considered as the tool rather than the target. These crimes generally involve less technical expertise as the damage done manifests itself in the real world. Human weaknesses are generally exploited. The damage dealt is largely psychological and intangible, making legal action against the variants more difficult. These are the crimes which have existed for centuries in the offline. Scams, theft, and the likes have existed even before the development in high-tech equipment. The same criminal has simply been given a tool which increases his potential pool of victims and makes him all the harder to trace and apprehend.

2) Computer as a target

These crimes are committed by a selected group of criminals. Unlike crimes using the computer as a tool, these crimes require the technical knowledge of the perpetrators. These crimes are relatively new, having been in existence for only as long as computers have - which explains how unprepared society and the world in general is towards combating these crimes. There are numerous crimes of this nature committed daily on the internet.

3) Fraud & Financial Crimes

Computer fraud is any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss. In this context, the fraud will result in obtaining a benefit by:

- 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. This is difficult to detect;
- Altering or deleting stored data;
- Altering or misusing existing system tools or software packages, or altering or writing code for fraudulent purposes.

Other forms of fraud may be facilitated using computer systems, including bank fraud, identity theft, extortion, and theft of classified information.

A variety of Internet scams target direct to consumers.

4) Obscene or offensive content

The content of websites and other electronic communications may be distasteful, obscene or offensive for a variety of reasons. In some instances these communications may be illegal.

The extent to which these communications are unlawful varies greatly between countries, and even within nations. It is a sensitive area in which the courts can become involved in arbitrating between groups with strong beliefs.

One area of Internet pornography that has been the target of the strongest efforts at curtailment is child pornography.

5) Harassment

Whereas content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing for example on gender, race, religion, nationality, sexual orientation. This often occurs in chat rooms, through newsgroups, and by sending hate e-mail to interested parties (see cyber bullying, cyber stalking, hate crime, Online predator, and stalking). Any comment that may be found derogatory or offensive is considered harassment.

There are instances where committing a crime, which involves the use of a computer, can lead to an enhanced sentence. For example, in the case of United States v. Neil Scott Kramer, Kramer was served an enhanced sentence according to the U.S. Sentencing Guidelines Manual §2G1.3(b)(3) for his use of a cell phone to “persuade, induce, entice, coerce, or facilitate the travel of, the minor to engage in prohibited sexual conduct.” Kramer argued that this claim was insufficient because his charge included persuading through a computer device and his cellular phone technically is not a computer. Although Kramer tried to argue this point, U.S. Sentencing Guidelines Manual states that the term computer "means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

Connecticut was the first state to pass a statute making it a criminal offense to harass someone by computer. Michigan, Arizona, and Virginia have also passed laws banning harassment by electronic means.

Harassment as defined in the U.S. computer statutes is typically distinct from cyber bullying, in that the former usually relates to a person's "use a computer or computer network to communicate obscene, vulgar, profane, lewd, lascivious, or indecent language, or make any suggestion or proposal of an obscene nature, or threaten any illegal or immoral act," while the latter need not involve anything of a sexual nature.

6) Threats

Although freedom of speech is protected by law in most democratic societies, it does not include all types of speech. In fact spoken or written "true threat" speech/text is criminalized because of "intent to harm or intimidate", that also applies for online or any type of network related threats in written text or speech. The US Supreme Court definition of "true threat" is "statements where the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence to a particular individual or group".

7) Drug trafficking

"Drug traffickers are increasingly taking advantage of the Internet" according to cyber authorities and personnel to sell their illegal substances through encrypted e-mail and other Internet Technology. Some drug traffickers arrange deals at internet cafes, use courier Web sites to track illegal packages of pills, and swap recipes for amphetamines in restricted-access chat rooms.

The rise in Internet drug trades could also be attributed to the lack of face-to-face communication. These virtual exchanges allow more intimidated individuals to more comfortably purchase illegal drugs. The sketchy effects that are often associated with drug trades are severely minimized and the filtering process that comes with physical interaction fades away.

8) Cyber terrorism

Government officials and Information Technology security specialists have documented a significant increase in Internet problems and server scans since early 2001. But there is a growing concern among federal officials that such intrusions are part of an organized effort by cyber terrorists, foreign intelligence services, or other groups to map potential security holes in critical systems. A cyber terrorist is someone who intimidates or coerces a government or organization to advance his or her political or social objectives by launching computer-based attack against computers, network, and the information stored on them.

Cyber terrorism in general, can be defined as an act of terrorism committed through the use of cyberspace or computer resources (Parker 1983). As such, a simple propaganda in the Internet, that there will be bomb attacks during the holidays can be considered cyberterrorism. As well there are also hacking activities directed towards individuals, families, organized by groups within networks, tending to cause fear among people, demonstrate power, collecting information relevant for ruining peoples' lives, robberies, blackmailing etc.

Cyber extortion is a form of cyber terrorism in which a website, e-mail server, or computer system is subjected to repeated denial of service or other attacks by malicious hackers, who demand money in return for promising to stop the attacks. According to the Federal Bureau of Investigation, cyber extortionists are increasingly attacking corporate websites and networks, crippling their ability to operate and demanding payments to restore their service. More than 20 cases are reported each month to the FBI and many go unreported in order to keep the victim's name out of the public domain. Perpetrators typically use a distributed denial-of-service attack.

IV. COMBATING CYBER CRIME

A computer can be a source of evidence. Even where a computer is not directly used for criminal purposes, it may contain records of value to criminal investigators in the form of a logfile. In most countries Internet Service Providers are required, by law, to keep their logfiles for a predetermined amount of time. For example; a European wide directive states that all E-mail traffic should be retained for a minimum of 12 months.

Penalties for computer related crimes in New York State can range from a fine and a short period of jail time for a Class A misdemeanor such as unauthorized use of a computer up to computer tampering in the first degree which is a Class C felony and can carry 3 to 15 years in prison.

V. REFERENCES

[1]. Moore, R. (2005) “Cyber crime: Investigating High-Technology Computer Crime” Cleveland, Mississippi: Anderson Publishing.

[2]. Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. p. 392.

[3]. David Mann And Mike Sutton (2011-11-06). “Netcrime”

[4]. Halder, D., & Jaishankar, K. (2011) Cyber crime and the Victimization of Women: Laws, Rights, and Regulation. Hershey, PA, USA: IGI Global.