ISSN No. 0976-5697

Volume 2, No. 5, Sept-Oct 2011

International Journal of Advanced Research in Computer Science

CASE STUDY AND REPORT

Available Online at www.ijarcs.info

Cyber Crime in India

Susheel Chandra Bhatt*
Computer Science department
SSJ Campus, Almora
Kumaun University, Nainital, Uttarakhand, India
bhatt.susheel@gmail.com

Durgesh Pant
Prof. & Director, School of Computer Science & IT
Uttarakhand Open University
Haldwani, India
durgesh_pant@yahoo.com

Abstract: Cyber crime is an evil having its origin in the growing dependence on computers in modern life. Computers and informatics have undoubtedly brought in remarkable transformation at all levels. The world, as we witness today, is not the same world what it was before the arrival of Internet and subsequently WWW. It totally changed and become popular as a cyber world. This cyber world is surrounded by number of things in which crime is the most serious threat. This paper is an attempt to provide a glimpse on cyber crime in India. This paper is based on various reports from web, newspaper and media.

Keywords: Security, Technology, Crime, Phishing, Cyber Stalking

I. INTRODUCTION

The increasing popularity of the internet has also spurred illegal activities. With the help of internet any one can visit the whole world by a single click of mouse. There is no specific boundary for anyone. This all thing is possible because of the technology and the different gadgets we are using made by the new technology. Combination of different gadgets, devices, technology, internet finally known as cyber world. Using this cyber world online transmission of electronic data, electronic commerce, electronic communication as well as electronic governance and mobile communication have become much popular worldwide which have attracted everyone. Government also changed their nature of work into electronic governance and information technology has become need of today. On the other hand Internet, though offers great benefit to society, also present opportunities for crime using new and highly sophisticated technology tools.

Cyberspace has no specific jurisdiction; therefore, criminals can commit crime from any location through computer in the world leaving no evidence to control [1]. Today e-mail and websites have become the preferred means of communication. Organizations provide Internet access to their staff. By their very nature, they facilitate almost instant exchange and dissemination of data, images and variety of material. This includes not only educational and informative material but also information that might be undesirable or anti-social. Regular stories featured in the media on computer crime include topics covering hacking to viruses, web-jackers, to internet paedophiles, sometimes accurately portraying events, sometimes misconceiving the role of technology in such activities. Increase in cyber crime rate has been documented in the news media. Both the increase in the incidence of criminal activity and the possible emergence of new varieties of criminal activity pose challenges for legal systems, as well as for law enforcement. Cyber crimes have been reported across the world. Cyber crime is now amongst the most important revenue sectors for global organized crime, says Frost & Sullivan Industry analyst Katie Gotzen.

Because of this, the potential risks associated with malware have risen dramatically. Unlike in traditional crimes, the Information Technology infrastructure is not only used to commit the crime but very often is itself the target of the crime [2]. This paper describes the various variants of cyber crime and also the scenario of cyber crime after 2001.

II. CYBER CRIME VARIANTS

In this section we are explaining various variants of technology that are used for cyber crime.

A. Hacking:

Hacking is unauthorized use of computer and network resources. The most prominent definition of hacking is the act of gaining access without legal authorization to a computer or computer network. A hacker first attacks an easy target, and then uses it to hide his or her traces for launching attacks at more secure sites. The goal of an attack is to gain complete control of the system (so he can edit, delete, install, or execute any file in any user's directory), often by gaining access to a "super-user" account. This will allow both maximum access and the ability to hide your presence. Early hackers needed to be very knowledgeable so that they were able to identify bugs themselves (a task requiring extensive knowledge about the operating system, and reading complex manuals) and often write their own programs to exploit them. They had to keep track of the leading developments in the field (latest bugs, latest patches, latest bugs in the patches, etc.). Later hackers were able to increasingly rely upon the hacking community to identify bugs and write programs that could be adapted for their specific purpose.

B. Phishing:

Phishing is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by illegally as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment

processors or IT administrators are commonly used to lure the unsuspecting public. Phishing is typically carried out by e-mail spoofing or instant messaging [3], and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users [4] and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures. A phishing technique was described in detail in 1987, and the first recorded use of the term "phishing" was made in 1996. The term is a variant of *fishing* [5] probably influenced by *phreaking* [6][7] and alludes to "baits" used in hopes that the potential victim will "bite" by clicking a malicious link or opening a malicious attachment, in which case their financial information and passwords may then be stolen. Not all phishing attacks require a fake website. Messages that claimed to be from a bank told users to dial a phone number regarding problems with their bank accounts [8]. Once the phone number (owned by the phisher, and provided by a Voice over IP service) was dialed, prompts told users to enter their account numbers and PIN. Vishing (voice phishing) sometimes uses fake caller-ID data to give the appearance that calls come from a trusted organization [9].

C. Spamming:

Spam is the use of electronic messaging systems (including most broadcast media, digital delivery systems) to send unsolicited bulk messages indiscriminately. The most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, online classified ads spam, mobile phone messaging spam, Internet forum spam, social networking spam. Spamming remains economically viable because advertisers have no operating costs beyond the management of their mailing lists, and it is difficult to hold senders accountable for their mass mailings. Because the barrier to entry is so low, spammers are numerous, and the volume of unsolicited mail has become very high. In the year 2011, the estimated figure for spam messages is around seven trillion. The costs, such as lost productivity and fraud, are borne by the public and by Internet service providers, which have been forced to add extra capacity to cope with the deluge. Spamming has been the subject of legislation in many jurisdictions [10].

D. Cyber Stalking:

Cyber stalking is the use of the Internet or other electronic means to stalk or harass an individual, a group of individuals, or an organization. It may include false accusations, monitoring, making threats, identity theft, and damage to data or equipment, the solicitation of minors for sex, or gathering information in order to harass. Technology ethics professor Lambèr Royakkers writes that: "Stalking is a form of mental assault, in which the perpetrator repeatedly, unwantedly, and disruptively breaks into the life-world of the victim, with whom he has no relationship (or no longer has), with motives that are directly or indirectly traceable to the affective sphere. Moreover, the separated acts that make up the intrusion cannot by themselves cause the mental abuse, but do taken together (cumulative effect) [11]."

E. Cyber Defamation:

Cyber Defamation is a crime conducted in cyberspace, usually through the Internet, with the intention of defaming others. Defamation is injury to the reputation of a person. If a person injures the reputation of another, he does so at his own risk, as in the case of an interference with the property. A man's reputation is his property, and if possible, more valuable than the other property. Cyber defamation is not different from conventional defamation except the involvement of a virtual medium.

F. Cyber Terrorism:

Cyber terrorism is the use of Internet based attacks in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses. Cyber terrorism can also be defined much more generally as any computer crime targeting computer networks without necessarily affecting real world infrastructure, property, or lives. The use of information technology by terrorist groups and individuals to further their goal. This can include use of information technology to organize and execute attacks against networks, computer systems and telecommunications infrastructures, or for exchanging information or making threats electronically. Examples are hacking into computer systems, introducing viruses to vulnerable networks, web site defacing, denial-of-service attacks, or terroristic threats made via electronic communication. Cyber terrorism can also include attacks on Internet business, but when this is done for economic motivations rather than ideological, it is typically regarded as cybercrime.

G. Cyber Pornography:

Cyber pornography is pornography that is distributed by means of various sectors of the Internet, primarily via websites, file sharing, or Usenet newsgroups. While pornography had been traded over the Internet since the 1980s, it was the invention of the World Wide Web in 1991 as well as the opening of the Internet to the general public around the same time that led to an explosion in online pornography. Like videotapes and DVDs, the Internet has proved popular for distributing pornography because it allows people to view pornography more or less anonymously in the comfort and privacy of their homes. It also allows access to pornography by people whose access is otherwise restricted for legal or social reasons. Pornography is often considered as one of the driving forces behind the early expansion of the World Wide Web. Pornographic images had been transmitted over the Internet as ASCII porn but to send images over network needed computers with graphics capability and also higher network bandwidth.

This was possible in the late '80s and early '90s through the use of anonymous FTP servers and through Gopher. This small image archive contained some low quality scanned pornographic images that were initially available to anyone anonymously. Usenet newsgroups also provided a way of sharing images over the narrow bandwidth available in the early 1990s. Images scanned from adult magazines were encoded as ASCII text and then broken into sections which were posted to the Alt.Binaries hierarchy of Usenet. These files could then be downloaded and then

reassembled before being decoded back to the images. Automated software such as aub allowed the automatic download and assembly of all the images from a newsgroup. There was a rapid growth in the number of posts in the early '90s but image quality was restricted by the size of files that could be posted. This type of distribution was generally free (apart from fees for Internet access), and provided a great deal of anonymity. The anonymity made it safe and easy to ignore copyright restrictions, as well as protecting the identity of uploaders and downloaders.

We must ensure that our system provides for stringent punishment of cybercrimes and cyber criminals so that the same acts as a deterrent for others. The Information Technology (IT) Act, 2008, specifies the acts which have been made punishable. Since the primary objective of this Act is to create an enabling environment for commercial use of I.T., certain omissions and commissions of criminals while using computers have not been included. With the legal recognition of Electronic Records and the amendments made in the several sections of the IPC vide the IT Act, 2008 several offences having bearing on cyber-arena are also registered under the appropriate sections of the IPC.

Table I. Reported Cases

Variants	*2001*	*2002*	*2003*	*2004*	*2005*	*2006*	*2007*	*2008*	*2009*	*2010*	*2011 (June)*
Hacking	12	25	20	35	45	39	75	87	123	145	109
Phishing	08	14	26	54	40	58	103	92	97	109	74
Spamming	04	17	19	29	43	67	86	94	89	105	57
Stalking	02	08	06	15	19	27	34	29	47	58	36
Defamation	03	11	09	13	17	24	32	37	59	46	45
Pornography	Nil	Nil	02	07	03	23	27	15	35	42	31

III. CYBER CRIME (2001 TO 2011)

Crime is no longer limited to space, time or a group of people. Cyber space creates moral, civil and criminal wrongs. It has now given a new way to express criminal tendencies. Back in 1990, less than 100,000 people were able to log on to the Internet worldwide. Now around 1000 million people are hooked up to surf the net around the globe. The latest statistics show that cybercrime is actually on the rise. However, it is true that in India, cybercrime is not reported too much about. Consequently there is a false sense of complacency that cybercrime does not exist and that society is safe from cybercrime. This is not the correct picture. The fact is that people in our country do not report cybercrimes for many reasons. Many do not want to face harassment by the police. There is also the fear of bad publicity in the media, which could hurt their reputation and standing in society. Also, it becomes extremely difficult to convince the police to register any cybercrime, because of lack of orientation and awareness about cybercrimes and their registration and handling by the police [12]. A recent survey indicates that for every 500 cybercrime incidents that take place, only 50 are reported to the police and out of that only one is actually registered. These figures indicate how difficult it is to convince the police to register a cybercrime.
The establishment of cybercrime cells in different parts of the country was expected to boost cybercrime reporting and prosecution. However, these cells haven't quite kept up with expectations. Peoples should not be under the impression that cybercrime is vanishing and they must realize that with each passing day, cyberspace becomes a more dangerous place to be in, where criminals roam freely to execute their criminals intentions encouraged by the so called anonymity that internet provides. The absolutely poor rate of cyber crime conviction in the country has also not helped the cause of regulating cybercrime. There have only been few cybercrime convictions in the whole country, which can be counted on fingers. We need to ensure that we have specialized procedures for prosecution of cybercrime cases so as to tackle them on a priority basis. This is necessary so as to win the faith of the people in the ability of the system to tackle cybercrime.

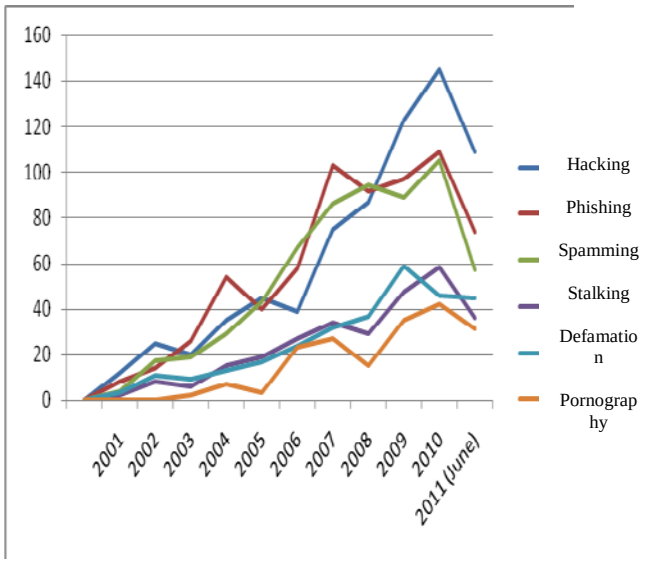

Figure 1. Graphical representation of Reported cases

Here we make a study on different variants of cyber crime from 2001 to 2011. We try to find out how these all variants are raising day by day and how they are affecting a common man. All the data are gathered from the news media as well as from the different web portal. In this study we found that the cyber crime is spreading rapidly. We can say from the data which we collected the growth is increasing year by year rapidly and these new kind of crime affecting society in different manner. In the early years the growth rate of reported cases was not so high but after 2005 the growth rate of reported cases is increasing suddenly. It doesn't mean before 2005 the cyber crime rate was very low. At that time the people was not much aware of that kind of crime. So if any incident was happened at that time it becomes extremely difficult to convince the police to register any cybercrime. Now this entire thing is possible because today peoples are much more aware and the police also accept this kind of thing is possible. Today there are number of Cyber police station is establishing by the government to report these kinds of crimes. Government also giving training to police

personnel's for handling cyber crimes. The latest technology is also helping the criminals to do crime easily. This is the more important factor of increasing cyber crime. Users are losing money, missing his personal information, harassing by anyone and number of things is happening in this cyber world. This paper show what is the current scenario of cyber crime in India and interesting thing is that this scenario is increasing rapidly because we can't stop the crime, we have to face this. The only one thing which we can do is prevention. We have to learn how to prevent by this kind of crime.

IV. CONCLUSION

In this paper we describe the different variants of cyber crime and also the scenario of cyber crime in last decade. We found that the growth rate is increasing day by day and affecting the human society in large scale. These kinds of crime are more dangerous comparison to conventional crime because the invisible crime is more dangerous than the visible one. We people are developing the latest technology by which we are trying to create a new era but we also have to aware because the same technology is also using in negative manner by some of the great minds. We can prevent himself and the society by spreading the awareness. We have to aware about the technologies which we are using and also need to increase our awareness level to secure humankind.

V. ACKNOWLEDGMENT

I would like to thank to Dr. Durgesh Pant, Prof. & Director at Uttarakhand Open University, India for supervising this research paper and is gratefully acknowledged.

VI. REFERENCES

[1] Cyber Crimes: A New Challenge, Deputy Controller (Technology), CCA, Ministry of Information Technology, India, 2002.

[2] (2008) Cyber Crime Scenario in India http://www.gcl.in/downloads/bm_cybercrime.pdf.

[3] Tan, Koontorm Center. "Phishing and Spamming via IM (SPIM)". Retrieved December 5, 2006.

[4] Microsoft Corporation. "What is social engineering?" Retrieved August 22, 2007.

[5] "Spam Slayer: Do You Speak Spam?". PCWorld.com. Retrieved August 16, 2006

[6] "Phishing, n. OED Online, March 2006, Oxford University Press.". Oxford English Dictionary Online. Retrieved August 9, 2006

[7] "Phishing". Language Log, September 22, 2004. Retrieved August 9, 2006.

[8] Gonsalves, Antone (April 25, 2006). "Phishers Snare Victims With VoIP". Techweb.

[9] "Identity thieves take advantage of VoIP". Silicon.com. March 21, 2005.

[10] The Spamhaus Project - The Definition Of Spam.

[11] Royakkers 2000:7, cited in CyberStalking: menaced on the internet.

[12] http://delhicourts.nic.in/CYBER%20LAW.pdf