Dr.B.Muthukumaran,
Chief Consultant,
Gemini Communication Ltd.,

CYBER CRIME SCENARIO IN INDIA

Abstract

Cyber crime is emerging as a serious threat. World wide governments, police departments and intelligence units have started to react. Initiatives to curb cross border cyber threats are taking shape. Indian police has initiated special cyber cells across the country and have started educating the personnel. This article is an attempt to provide a glimpse on cyber crime in India. This article is based on various reports from news ***media*** *and news portal.* **Key words**

Cyber crime, Hacking, Phishing, Vishing, Cyber squatting 1. Introduction

The world of Internet today has become a parallel form of life and living. Public are now capable of doing things which were not imaginable few years ago. The Internet is fast becoming a way of life for millions of people and also a way of living because of growing dependence and reliance of the mankind on these machines. Internet has enabled the use of website communication, email and a lot of any time anywhere IT solutions for the betterment of human kind.

Internet, though offers great benefit to society, also present opportunities for crime using new and highly sophisticated technology tools. 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-j ackers, 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. 2. **Cyber** Space ~ cyber **crime**

Cyber space is a collective noun for the diverse range of environments that have arisen using the Internet and the various services.

The expression **crime** is defined as an act, which subjects the doer to legal punishment or any offence against morality, social order or any unjust or shameful act. The "offence" is defined in the Code of Criminal Procedure to mean as an act or omission made punishable by any law for the time being in force.

Cyber crime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity. **3. Traditional** crime - **Cyber Crime**

Computer crime mainly consists of unauthorized access to computer systems data alteration, data destruction, theft of intellectual properly. Cyber crime in the context of national security may involve hacktivism, traditional espionage, or information warfare and related activities.

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. Pornography, threatening email, assuming someone's identity, sexual harassment, defamation, SPAM and Phishing are some examples where computers are used to commit crime, whereas viruses, worms and industrial espionage, software piracy and hacking are examples where computers become target of crime.

There are two sides to cyber crime. One is the generation side and the other is the victimization side. Ultimately they have to be reconciled in that, the number of cyber crimes committed should be related to the number of victimizations experienced. Of course there will not be a one-to-one correspondence since one crime may, inflict multiple victimizations multiple crimes may be responsible for a single victimization. Some crimes may not result in any victimization, or at least in any measurable or identifiable victimization.

The obvious effect of cyber crime on business is the evolving threat landscape. 'The motive of the attacks has changed over time. Earlier, the intent of the attacker was to gain fame although the motivation was criminal. Cyber crime economics are too compelling to subside. **4. Cyber Crime variants**

There are a good number of cyber crime variants. A few varieties are discussed for the purpose of completion. Thi s article is not intended to expose all the variants. The readers are directed to other resources.

4.1 Cyber stalking

Cyber stalking is use of the Internet or other electronic means to stalk someone. This term is used interchangeably with online harassment and online abuse. Stalking generally involves harassing or threatening behavior that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property.

4.2 Hacking

"Hacking" is a crime, which entails cracking systems and gaining unauthorized access to the data stored in them. Hacking had witnessed a 37 per cent increase this year

4.3 Phishing

Phishing is just one of the many frauds on the Internet, trying to fool people into parting with their money. Phishing refers to the receipt of unsolicited emails by customers of financial institutions, requesting them to enter their username, password or other personal information to access their account for some reason. Customers are directed to a fraudulent replica of the original institution's website when they click on the links on the email to enter their information, and so they remain unaware that the fraud has occurred. The fraudster then has access to the customer's online bank account and to the funds contained in that account.

F-Secure Corporation's summary of 'data security' threats during the first half of 2007 has revealed that the study found the banking industry as soft target for phishing scams in India [The Business line Monday July 23 2007J

4.4 cross **site scripting**

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications which allow code injection by malicious web users into the web pages viewed by other users. Examples of such code include HTML code and client-side scripts. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls.

4.5 Vishing

Vishing is the criminal practice of using social engineering and Voice over IP (VoIP) to gain access to private .personal and financial i nformation from the public for the purpose of financial reward. The term is a combination of "voice" and phishing. Vishing exploits the public's

trust in landline telephone services, which have traditionally terminated in physical locations which are known to the telephone company, and associated with a bill-payer. The victim is often unaware that VoIP allows for caller ID spoofing, inexpensive, complex automated systems and anonymity for the bill-payer. Vishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals.

4.6 Cyber Squatting

Cyber squatting is the act of registering a famous domain name and then selling it for a fortune. This is an issue that has not been tackled in IT act 2000.

4.7 Bot Networks

A cyber crime called 'Bot Networks', wherein spamsters and other perpetrators of cyber crimes remotely take control of computers without the users realizing it, is increasing at an alarming rate. Computers get linked to Bot Networks when users unknowingly download malicious codes such as Trojan horse sent as e-mail attachments. Such affected computers, known as zombies, can work together whenever the malicious code within them get activated, and those who are behind the Bot Neworks attacks get the computing powers of thousands of systems at their disposal. Attackers often coordinate large groups of Bot-controlled systems, or Bot networks, to scan for vulnerable systems and use them to increase the speed and breadth of their attacks.

Trojan horse provides a backdoor to the computers acquired. A 'backdoor" is a method of bypassing normal authentication, or of securing remote access to a computer, while attempting to remain hidden from casual inspection. The backdoor may take the form of an installed program, or could be a modification to a legitimate program.

Bot networks create unique problems for organisations because they can be remotely upgraded with new exploits very quickly," and this could help attackers pre-empt security efforts.

5. Vulnerability

The Open-Source Vulnerability Database (OSVDB) project maintains a master list of computer - security vulnerabilities, freely available for use by security professionals and projects around the world. Vulnerability information is critical for the protection of information systems everywhere: in enterprises and other organizations, on private networks and intranets, and on the public Internet.

6. Indian Crime Scene

The major cyber crimes reported, in India, are denial of services, defacement of websites, **SPAM,** computer virus and worms, pornography, cyber squatting, cyber stalking and phishing.[l]

Given the fact that nearly $ 120 million worth of mobiles are being lost or stolen in the country every year, the users have to protect information, contact details and telephone numbers as these could be misused. Nearly 69 per cent of information theft is carried out by current and ex-employees and 31 per cent by hackers. India has to go a long way in protecting the vital information. [3 The Hindu, Saturday, Oct 27,2007].

Symantec shares the numbers from its first systematic survey carried out on the Indian Net Security scene: The country has the highest ratio in the world (76 per cent) of outgoing spam or junk mail, to legitimate e-mail traffic. India's home PC owners are the most targeted sector of its 37.7 million Internet users: Over 86 per cent of all attacks, mostly via 'bots' were aimed at lay surfers with Mumbai and Delhi emerging as the top two cities for such vulnerability.

6.1 Phishing

Phishing attacks were more popular among Indian users due to rising Internet penetration and growing online transactions. India has now joined the dubious list of the world's top 15 countries hosting "phishing" sites which aims at stealing confidential information such as passwords and credit card details. [The Hindu Sunday Nov 26 2006]

A non-resident Malayali, had an account in a nationalized bank in Adoor, lost $ 10,000 when the bank authorities heeded a fake e-mail request to transfer the amount to an account in Ghana. In Mangalapuram, a person transferred a large sum of money as "processing charge" to a foreign bank account after he received an e-mail, which said he had won a lottery LKerala: The Hindu Monday Oct 30 2006] Reports of phishing targeted at customers of banks appear to be on the rise. Websense Security Labs, in a statement released recently, said it had received reports of such attacks from customers of AXIS Bank. The Economic Offences Wing (EOW), Crime Branch, Delhi Police, unearthed a major phishing scam involving fake emails and websites of UT1 Bank, An analysis of the accounts of the four arrested Nigerian nationals

- c

indicated financial transactions of over Rs 1 crore in an eight-month period till December 2006. Investigations revealed that the scam is multi-layered with pan-India and international characteristics The Lab went on to say that it found a mal ware in the Web site of Syndicate Bank. The users through a spoofed email were asked to renew certain services and claiming that failure to do so would result in suspension or deletion of the account. The e-mail provided a link to a malicious site that attempted to capture the personal and account information. [The Hindu, Monday August 20 2007].

Phishing emails have increased by approximately twenty five percent over the last year but are harder to detect as they increasingly trick unsuspecting people with ordinary scenarios instead of improbable ones such as sudden cash windfalls.

It has been six months since the phishing attack on ICICI bank customers became public, and during that period, two more such attacks were reported on customers of financial institutions in India, one of UTI Bank and the other. State Bank oflndia. [5-Jan 17-theHindu]

RSA's 24/7 Anti-Fraud Command Centre f AFCC) has just uncovered a 'Universal man-in-the-middle Phishing Kit' in online forums which helps phishers quickly create the fraudulent websites, often borrowing code from the original site. [The Hindu Wednesday, Jan 17 2007] **6.2 Cyber Cafes ~ Emails**

Cyber cafes have emerged as hot spots for cyber crimes. Even terrorists prefer the anonymity of a cyber cafe to communicate with each other. The mushrooming of cyber cafes in the city, which provide the secrecy through cabins constructed for users, has also made the porn literature easily accessible to the people visiting them. (Chandigarh Tribune Monday May 28 2001] A 23-year-old person from Tiruchi was arrested by the City Cyber Crime police on Thursday on charges of sendi ng an e-mail threat to the Chief Minister and his family. [The Hindu Friday Aug 10 2007] In another case, the police team investigating the e-mail threat on the lives of the President and the Pri me M inister has prepared a sketch of the suspect, who had sent the email from a cyber cafe in the city. [The Hindu, Sunday Ocober292006].

The Case of The State of Tamil Nadu Vs Suhas Katti is notable for the fact that the conviction was achieved successfully. The case related to posting of obscene, defamatory and annoying message about a divorcee woman in the yahoo message group. E-Mails were also forwarded to the victim for information by the accused through a false e-mail account opened by him in the name of the victim. The posting of the message resulted in annoying phone calls to the lady.

A travel agent was arrested for allegedly sending a threatening mail to blow up the National and Bombay stock exchanges in Kolkata [Express India.com Sun 28 Oct 2007]. 6.3 **Stalking**

A tenth standard boy from Bangalore got into trouble when a girl much older than him started stalking him. She pasted T Love You' slips on his gate and called his

"On reviewing his Orkut profile, it was realized that he had accepted chat invites from more than 20 people; only two of who were his real-life friends. [The Hindu Tuesday, May 01, 2007] **6.4 Hacking**

A case of suspected hacking of certain web portals and obtaining the residential addresses from the e-mail accounts of city residents had recently come to light. After getting the addresses, letters were sent through post mail and the recipients were lured into participating in an international lottery that had Australian $ 23 lakhs at stake.

Computer hackers have also got into the Bhaba Atomic Research Centre (BARC) computer and pulled out important data. Some computer professionals who prepared the software for MBBS examination altered the data and gave an upward

- **revision** to some students in return for

a hefty payment.

A key finding of the Economic Crime Survey 2006 of Price waterhouseCoopers (PwC) was that a typical perpetrator of economic crime in India was male (almost 100 per cent), a graduate or undergraduate and 31-50 years of age. Further, over one-third of the frauds in the country were perpetrated by insiders and over 37 per cent of them were in senior managerial positions.

father to express her love for the son.

7. **Global AntiMalware Market**

Malware is software designed to infiltrate or damage a computer system without the owner's informed consent. The expression is ageneral term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

The global anti-malware market is driven by cyber criminal threats. The commercialisation of cyber crime is spurring malware-writing activity and leading to more threats of this nature. In the consumer space, this translates into identity theft and stolen passwords Growth opportunities have led to intensified competition in both consumer and enterprise segments. On the other hand, loss of intellectual property and customer data coupled with extortion with the threat of taking down Web sites or revealing sensitive information are on the rise in the enterprise space. Organised crime is now employing KGB-style tactics to ensnare the next generation of hackers and malware authors. Cyber-criminals are actively approaching students and graduates of IT technology courses to recruit a fresh wealth of cyber skill to their ranks

Today's worms are the **handiwork of** malcontents for whom **cyber** crime affords lucrative returns. A flourishing market exists where large blocks of infected machines that can be controlled remotely are for sale. Sobig demonstrated the close nexus between malware writers and spammers, machines infected by the Sobig mass mailing worm were offered to spammers for price.

The thriving market for subverted PCs has swung the underworld into hyperactivity. The past ten months have seen several hacker groups and cyber crime syndicates setting up attack networks (botnets) and releasing remote attack tools through increasingly crafty malware such as Blaster, Sinit, MyDoom, Phatbot, Bagle and Netsky.

New analysis from Frost & Sullivan, World Anti-Malware Products Markets, finds that the world market for antivirus solutions reached $4,685 million in 2006, up 17.1 per cent from $4,000.7 million in the previous year and expects this market to grow at a 10.9 per cent compound annual growth rate (CAGR) from 2006 to 2013, reaching $9,689.7 million by 2013.

8. Anti Cyber crime **Initiatives**

In a first of its kind initiative in India to tackle cyber crime, police have taken the initiative to keep an electronic eye on the users of the various cyber cafes spread over the city. The Kerala State IT Mission has

launched a Web portal and a call centre to tackle cyber crime. [The

Hindu Business line, Tuesday, Jul 31, 2007]. The Central Bureau of Investigation (CBI) and the Mumbai police have recommended issuance of licenses to cyber cafe owners. Many countries, including India, have established Computer Emergency Response Teams (CERTs) with an objective to coordinate and respond during major security incidents/events. These organisations identify and address existing and potential threats and vulnerabilities in the system and coordinate with stakeholders to address these threats.

Policy initiatives on cyber crime are as yet lethargic because of a general sense that it is nothing more than juvenile hackers out to have fun or impress someone. . Prateek Bhargava, cyber law expert says, "There is huge potential for damage to national security through cyber attacks. The internet is a means for money laundering and funding terrorist attacks in an organized manner. In the words of Pavan Duggal, Supreme Court Lawyer, "Cyber crime is omnipresent and although cyber crime cells have been set up in major cities, most cases remain unreported due to lack of awareness." 9. Conclusion

'Net surfing[1] by youngsters lures them into dangerous domain. The need for a conscious effort to checkmate the undesirable fallout of youngsters accessing and using the Internet is of concern. The print media has a duty to educate unwary parents and youngsters about the dangers inherent in treading dangerous areas in the cyber-world.

Cyber Space Security Management has already become an important component of National Security Management, Military-related Scientific Security Management and Intelligence Management all over the world. Future intrusions threatening our national security may not necessarily come from across the land frontier, or in air space or across maritime waters, but happen in eyberspace. Intelligence operations and covert actions will increasingly become cyber-based. It is important that our intelligence agencies gear themselves up to this new threat. It is, therefore, necessary to put in place a 'National Cyber Space Security Management Policy' to define the tasks, specify responsibilities of individual agencies with an integrated architecture.

It is a well-known fact that terrorists have been using the Internet to communicate, extort, intimidate, raise funds and coordinate operations. Hostile states have highly developed capabilities to wage cyber wars. They have the capability to paralyse large parts of communication networks, cause financial meltdown and unrest. The degree of our preparedness in the face of all these potential threats, does leaves much to be desired. The Government should also take note of this slow but worrying development and put in place a proper mechanism to curb the misuse.

Reference

$• Cyber Crime Today & Tomorrow, Thiru Dayanithi Maran, http://www.d.maran.nic.in/speechdisplay.ph,p?jd=i?9 [viewed on 27-10-2007]

-$- Police make headway, The Hindu, Sunday Ocober 29 2006.

•$• Cyber Crimes on the rise in state - Kerala: The Hindu Monday Oct 30 2006

-$- Nowa Pune base for net's cyber cops The Hindu Sunday Nov 26 2006

0- Bank Customers face Phishing, The hindu, Coimbatore, Monday August 20 2007,

•$• Phishing attacks against Indians: F-Secure, The Business line Monday July 232007

Tamil Nadu to come out with ^ IT security policy soon, The Hindu, Saturday, Oct 27, 2007

Youth in jail for sending email •£ threat TheHindu Friday Aug 102007

Phishing for trouble: The hindu Wednesday, Jan 17 2007 ^

Cyber crime Up Police found wanting, Chandigarh Tribune Monday May 28 2001

Nasik Police play big bossfor internet voyeurs, Hindustan Times, Sunday, Oct 28 2007

Losses due to cyber crime can be as high as $40 billion, The Hindu Business line dt May 21 2007 downloaded 20 Oct2007

Kolkata man threatens to blow up Stock exchanges arrested. Express India.com Sun 28 Oct 2007

Suhas Shetty Cyber Crime Case, First conviction in India under ITA-2000. http://www.naavi.org/cl_editorial_04/suhas_katti_case.htm

Web portal Call center to tackle cyber crime, The Hindu Business line, Tuesday, Jul 31,2007

Licenses mooted for Internet Cafes, The Hindu Business line Saturday, Aug 23,2(Xb

Look Whos stalking? The Hindu Tuesday, May 01, 2007.