Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

3G Widens the Scope for Cyber Crime in India

Vivek Saini[1] and Ashok Kumar Saini[2]

[1] NIMS University Jaipur Rajasthan

Received: 5 April 2012 Accepted: 5 May 2012 Published: 15 May 2012

Abstract

The revolutionary decline in price and complexity of computers, laptops and mobile phone has changed the whole statistics of internet users. Considerable decline in price of internet charges also has contributed to the gigantic rise up of the curve of internet users. 3G introduction in India has act as a catalyst to the phenomena of rising the rectangular boxes in recent two or three year, so as the index of Cyber Crime.

Index terms— Cyber crime, 3G, India, virus, threats

the vulnerability. Through a technique called 'smishing' a hacker will send an SMS to the target, enticing him to click on a web link. Upon clicking the link, malware gets downloaded and settles in the mobile phone memory, enabling the hacker to read all the data stored in the phone. a) Interesting Findings Of Norton Cybercrime Report 8% Indians do not expect to be cyber-crime victims ever as compared to 3% globally and 10% Indians feel that they are completely safe online.

57% Indians feel that cyber criminals will NOT be brought to justice as compared to 79% globally.

Once an individual has fallen prey to cybercrime, 58% of them change the way they conduct themselves online while very few individuals call Police or Banks to ensure safety! It takes average of 44 days and Rs. 5262 to resolve a cybercrime in India, while globally the average is 28 days and over USD 334 (Rs. 13500 approx.) 55% of Indian online users have lied about their personal details as compared to 45% globally. 36% Indians have used fake online IDs (33% globally)

19% of Indian regret as to what they have done previously online and 41% believe that once your online reputation is ruined, nothing can be done about it. **??** The daily update of new virus definitions from Symantec[5] is around 130MB and McAfee's [6] is around 120MB. On a 56Kb dialup link, this can take all day to download. Although this restriction can cause frustration, it is an inherent type of risk proofing. From a business point of view, higher Internet speeds equate to more data being vulnerable to theft and other types of cyber crime. -Over a slow Internet link, it might have taken days to transfer even one 1GB of stolen data, but with 3G, the same can happen in minutes. Generally, the faster the link, the higher the amount of threats that might come. Fig. 1 shows the 3G services provided in different states in India by major operators.

1 Docomo

Reliance Airtel Vodafone Aircel Idea Though the India is the second largest English speaking population in world. The absence of Indian languages in cyber space stands in direct relation to a shortage of IT education. It has a direct impact on the vulnerability of the Indian cyber space due to lack of cognizance.Though a mass of people have acquired computer skills, language is still a problem because the computer is dominated by English. In many instances, computer users willing to learn about cyber space are restricted to do this, because Indian languages are used minimally in cyber space. Many Indian computer users do not necessarily understand error messages or warnings about cyber fraud that are not presented in their mother tongue. As a result, the absence of Indian languages in cyber space poses a potentially serious threat to cyber space fraud and vulnerability to cyber space fraud. d) Third Party Application Vulnerabilities And Zero Day Exploits Third party applications are programs written to work within operating systems, but are written by individuals or companies other than the provider of the operating system. For example, Microsoft® systems come packed with several software applications. Of these, any program authored by Microsoft is a first party application. Any program authored by a different company or an individual is a third party application.

A zero-day (or zero-hour or day zero) attack or threat is a computer threat that tries to exploit computer application vulnerabilities that are unknown to others or the software developer. Zero-day exploits (actual software that uses a security hole to carry out an attack) are used or shared by attackers before the developer of the target software knows about the vulnerability.

The term derives from the age of the exploit. A ”zero day” attack occurs on or before the first or ”zeroth” day of developer awareness, meaning the developer has not had any opportunity to distribute a security fix to users of the software.

2 e) Social Engineering

Social engineering is commonly understood to mean the art of manipulating people into performing actions or divulging confidential information. While it is similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes faceto-face with the victims.

3 Global Journal of Computer Science and Technology Volume XII Issue IV Version I

4 F ebruary f) The Insider

The insider threat or insider problem is cited as the most serious security problem in many studies. It is also considered the most difficult problem to deal with, because an insider has information and capabilities not known to other, external attackers. But the studies rarely define what the insider threat is or define it nebulously. A system administrator at a bank accesses a financial system that she is responsible for. She notices that Rs. 100000 was transferred from account 1011 to account 6734. The account of a close friend is number 6834. She moves the money to her friend's account, alters the original log file entry to change the number to that of the friend's account, and deletes the log entries showing the money being moved from account 6734 to account 6834. This seems to qualify as -unauthorized access by an insider?. a) Smishing Through a technique called 'smishing' a hacker will send an SMS to the target, enticing him to click on a web link. Upon clicking the link, malware gets downloaded and settles in the mobile phone memory, enabling the hacker to read all the data stored in the phone. Cyber crime police have been receiving several complaints from women about people blackmailing them using the intimate videos captured on web or cell phone cameras. Police are apprehensive that if an individual is not careful, video calling facility can also be misused in similar manner. The hacker can record all the audio conversation and video files. Not many people in India install anti-virus in the phones. I would recommend them to install anti-virus and fireballs while using 3G and recommend switching off the bluetooth function of the phone when not required to protect the user's password. Due to high speed internet and lack of antiviruses in our system, crucial informations from our system can be easily hacked within seconds.

5 AIRTEL

6 c) Film And Music Industry

Not limited to an individual's privacy issues, the 3G technology will also lead to increase in piracy of films and music, thereby giving a staggering amount of losses to the entertainment industry that is battling the piracy threat.

”It will become extremely easy for anybody to download an entire Bollywood film in few minutes using 3G. This is going to lead to further tremendous growth of websites like torrents,” says advocate Pavan Duggal, a cyber-laws expert.

The Internet and Mobile Association of India (IAMAI) points out that Bollywood would be hit most by the 3G and wants service providers to adopt a stricter approach to check cybercrimes.

7 d) Absence Of Awareness Towards Internet

If we are to believe the official figures (1350 cybercrime cases in 2010 in India), then India is the most cyber secure country in the world, which is utter nonsense. Internet users in the country need to be educated about cybercrime. In many cases they might not even know that they have been a victim of cybercrime. The particulars of the law need to be made common knowledge. Cyber bullying is rampant in chat rooms and social networks. Children are most exposed to it and often not aware of consequences. Symantec Corp's Norton Cybercrime Report 2011 reported that four in five online adults have been victims of cybercrime in India.

8 e) Cyberwarfare

Cyberwarfare refers to politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare, although this analogy is controversial for both its accuracy and its political motivation.

India has received many threats of penetrating in the government computers and Indian networks for the purpose of causing damage or disruption. In an electronically linked world, nations are increasingly connected economically. In a war, destruction will be more severe and fatal if the economy collapses. And the recovery process after the war will be long winding. With the increase in bandwidth the file transfer rate has been increased considerably. Hackers can now transfer more data in a single second. Now with the increased speed user can download third party applications with which he can have access to the others computers or mobile phones. Operating Systems with patches are also available on the internet. So in poor contries like India people can download pirated versions of operating system and third party software easily with the help of large bandwidth internet.

9 b) Influence Of 3G On Social Engineering

With the increase in bandwidth and more and more people are joining into the cyber world the individual information are more prone to be attacked. For example, a person want to get the personal information of an individual, he can get it by the social networking sites(facebook, orkut, myspace, twitter) by hacking the account of that individual. A fake social networking site login page is sent to the user with an attractive link so that by loging into that page can send the user name and password of that user to the hacker. The fake login page is developed to do the so.

10 c) Influence Of 3G On Viruses

With the increase in bandwidth and more and more people are joining into the cyber world may potentially increase in the viruses, trojen horses and spam. Hackers can easily get into the remote computers and can infect a whole network with in seconds with the faster access of internet. With new reports suggesting that 3G subscribers will cross 107 million users in India by 2015 and most of the users would be virus infected.

11 d) Influence Of 3G On Film And Music Industry

With the increase in bandwidth and more and more people are joining into the cyber world may potentially affact the growth of Film and Music Industry. With high speed internet user can download a whole movie into a few minutes and song can be downloaded into few seconds. This is increasing the piracy of movies and songs. As the revenue is flowing to the illegal sites rather than the producer of movie or the songs. e) Influence Of 3G On Cyberwarfare Now-a-days nations have electronically connected all their economic, defense and national security establishments which will be the target for cyber attacks during a conflict or to create instabilities. With the increase in 3G user access these sites are more prone to attack as hacker can have more bandwidth and can destruct in more networks in less time. This research identified many areas where there are currently deficiencies in India's law enforcement response to cyber crime. Researches has shown that there is high volume of malicious computer activities in India. It is impossible to take counter measures to defeat cyber crime in India. Here we are suggesting some counter measures to defeat cyber crime in India like Emergency Response Teams, Cyber Security Awareness Campaign etc. a) Cyber Space Initiative A number of cyber space initiatives has to be taken to combat cyber crime in India. Speaking at the golden jubilee function of Karnataka State Bar Council President Pratibha Patil said: -Technology has thrown up issues which were unheard of a few years ago, like cyber crime and hacking. How to deal with these will require new thinking and new knowledge.? Initiatives such as the International Telecommunication Union (ITU) High Level Expert Group (HLEG) aim to develop strategies and guidance to countries in dealing with cyber crime.

The CBI chief said that during Noble's discussion with CBI officials, "we have broadly agreed that a CBI-Interpol Research and Innovation Centre for Prevention of Telecommunication Crime would be established in India".

One cyber space intitiative is Setting up Digital Forensics Centres (Cyber Forensics) where domain specific training could be provided.

Another cyber space initiative is One Laptop per Child.This initiative is trying to create educational opportunities for the world's poorest children by providing each child with a rugged, low-cost, low-power, connected laptop with content and specifically designed software. [More information on this initiative can be found at http://www.olpcindia.net/] b) Indian Computer Emergency Response Team Computer Emergency Response Team is a name given to expert groups that handle computer security incidents. CERT-In is operational Since Januray 2004. The constituency of CERT-In is the Indian Cyber Community. CERT-In is the national nodal agency for responding to computer security incidents as and when they occur.

In the recent Information Technology Amendment Act 2008,CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security: Indian government should come out with a PPP (Public Private Partnership) model, which includes government, private organizations and NGOs to make people more aware of the cyber attacks and increase the level of security. Through collective efforts -such as the sharing of threat intelligence and guidance, software providers making advancements in security protections and customers keeping their systems up to date, using genuine sofwares, will surely help in minimizing cyber crime while delivering a more safer and reliable computing experience.

158 Although cyber-security awareness among the people in India is on the rise, there is ample scope to expand
159 awareness, which is possible through the PPP model.
160 The paper examines the relationship between high bandwidth internet and the cyber security issues. With
161 the rising number of cyber crimes, it is imperative to take specific counter measures to address crimes in cyber
162 space. An increase in broadband access will give Internet access to more users in India. With the increase in
163 broadband access, millions of new, computer-illiterate users will be able to connect to the internet through the
164 3G, potentially making the entire network more vulnerable to cyber threats and attacks.
165 Maintaining cyber security initiatives, establishing CERT-In and Cyber Security Awareness Campaign can
help India defeating the Cyber Crime. [1]

1

Figure 1: Fig. 1 b

Figure 2:

166

[1] © 2012 Global Journals Inc. (US) Global Journal of Computer Science and Technology Volume XII Issue IV Version I

Figure 3: ©

-

[Note: a) Bandwidth Availability]

Figure 4: Table - 1

-

c) Absence Of Indian Languages

Figure 5: Table - 2

2012
F ebruary
50
? Collection, analysis and dissemination of
information on cyber incidents.
? Forecast and alerts of cyber security incidents
? Emergency measures for handling cyber security
incidents
? Coordination of cyber incident response activities
? Issue guidelines,advisories,vulnerability notes and
whitepapers relating to information security
? Ractices, procedures, revention, response and
reporting of cyber incidents.
c) Cyber Security Awareness Campaign
For combating cyber crime, cyber security
awareness should be created among the computer
users in India. Department of Information Technology
(DIT),

Figure 6:

.1 Global Journals Inc. (US) Guidelines Handbook 2012

www.GlobalJournals.org

[International Journal of Cyber Criminology (IJCC) (2009)] , *International Journal of Cyber Criminology (IJCC)* 0974 -2891. July -December 2009. 3 (2) p. .

[Gordon et al. ()] *CSI/FBI Computer crime and security survey*, L Gordon , M Loeb , W Lucyshyn , R Richardson . http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf 2006.

[Hashimoto (2007)] 'Current issues and measures for prevention of cybercrime'. Naoki Hashimoto . *S?sa kenky? [Investigation research*, February 2007. 56 p. .

[Abe (2007)] *Current issues and measures for prevention of cybercrime?Prosecution of cybercrime*, Makoto Abe . February 2007. 62 p. . (Keisatsu jih? [Police times)

[Cyber Crime report 2011 by Norton Security] http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport/ *Cyber Crime report 2011 by Norton Security*,

[Billo and Chang] *Cyber Warfare-An analysis of the means and motivations of selected nation states*, Charles Billo , Welten Chang . http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf

[Daily updates of McAfee antivirus definitions] *Daily updates of McAfee antivirus definitions*, http://www.mcafee.com/apps/downloads/security-updates/security-updates.aspx

[Daily Updates of Symentec antivirus definitions] http://www.symantec.com/security_response/definitions/download/detail.jsp?gid=n95 *Daily Updates of Symentec antivirus definitions*,

[International trends in measures against cybercrime and the establishment of information security JISA Bulletin (2001)] 'International trends in measures against cybercrime and the establishment of information security'. *JISA Bulletin* October 2001. 63 p. . (Association for Information Service Industries: International Branch)

[On the prosecution of cybercrime Heisei 19th [19th Conference] f the National Police Agency ()]b11 'On the prosecution of cybercrime'. *Heisei 19th [19th Conference] of the National Police Agency*, 2008. National Police Agency

[Tariff plans for 3G services of various major telecom operators in India.URL-http:www.airtel.in, http:www.vodafone.in,http:www http:\char"005C\relax\char"005C\relaxwww.rcom.co.in *Tariff plans for 3G services of various major telecom operators in India.URL-http:\\www.airtel.in, http:\\www.vodafone.in,http:\\www.ideacellular.com*,

[URL-http:www India Internet Statistics Compendium (2010)] 'URL-http:\\www'. http://www.slideshare.net/Vicks18/orindia-internetstatistics-e-statsindiacom-compendium-january-2011-pdf *India Internet Statistics Compendium* 2010. January 2011.

[Babu and Parishat (2004)] *What is cyber crime*, M Babu , M G Parishat . http://www.crime-research.org/analytics/702/ 2004. November 10, 2009.