Dept of Computer Science, P B SIDDHARTHA COLLEGE OF ARTS & SCIENCE, VIJAYAWADA.
UGC SPONSORED NATIONAL SEMINAR ON "CYBER SECURITY WITH SPECIAL FOCUS ON CYBER CRIMES & CYBER LAWS (NSCS 2014)" on
15th & 16th November 2014-IJDCST SPECIAL ISSUE, PAPER –ID: IJDCST-02
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Cyber Crime in India: An Overview

Dr.M.Rajanikanth [1], Sri.Ch.Anilkumar [2]

[1]**Lecturer in Computer Science, V.S.R. Govt. Degree & P.G. College, Movva, Krishna District, A.P., India**

[2]**Lecturer in Computer Science, V.S.R. Govt. Degree & P.G. College, Movva, Krishna District, A.P., India**

Abstract: The advent of technological revolution in communications and information exchange has created sophisticated form of crime is called, cyber crime. Cybercrimes have more severe economic impacts than many conventional crimes and like any other crime. Cyber crimes are a new class of crimes rapidly increasing due to extensive use of Internet and I.T. enabled services. Through internet and WWW, anyone can access information at anytime and anywhere but the data which is available online can be targeted by third person in a way of hacking, pashing, etc. to harm the computer and information stored in computer or available online. This type of happening is called cyber crime. Cyber crime always involves some degree of infringement on the privacy of others or damage to computer-based property such as files, web pages or software. This paper deals with cybercrime in India and its crime statistics.

Keywords: Cyber Crime, hacking, phishing.

Introduction

Current era is too fast to utilize the time factor to improve the performance factor. It is only possible due the use of Internet. The term Internet can be defined as the collection of millions of computers that provide a network of electronic connections between the computers. There are millions of computers connected to the internet. Everyone appreciates the use of Internet but there is another side of the coin that is cyber crime by the use of Internet.

The term cyber crime can be defined as an act committed or omitted in violation of a law forbidding or commanding it and for which punishment is imposed upon conviction. Other words represents the cyber crime as ―Criminal activity directly related to the use of computers, specifically illegal trespass into the computer system or database of another, manipulation or theft of stored or on-line data, or sabotage of equipment and data.

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

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.

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.

ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

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.

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.

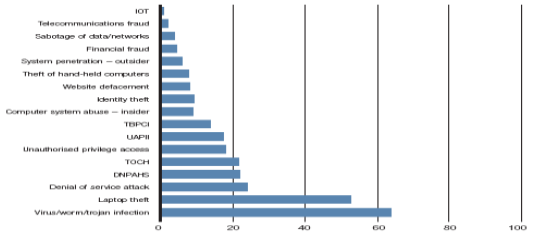
Vishing

Vishing is the criminal practice of using social engineering and Voice over IP (VoIP) to gain access to private .personal and financial Information 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 billpayer. Vishing is typically used tosteal credit card numbers or other information used in identity theft schemes from individuals.

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.

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 Networks attacks get the computing powers of thousands of systems at their disposal. Attackers often coordinate large groups of Bot-controlled systems, or Boot 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. Boot networks create unique problems for organizations because they can be

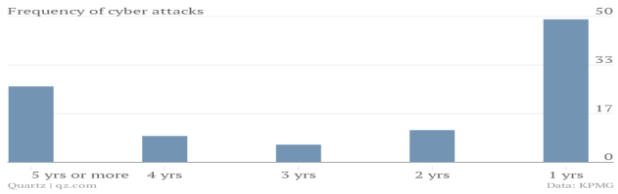
remotely upgraded with new exploits very quickly and this could help attackers pre-empt security efforts.



Frequency of cyber attacks

In the past, India used to be a target of cyber attacks for political motivation only. Over the past few years, the global cybercrime landscape has changed dramatically, with criminals employing more sophisticated technology and greater knowledge of cyber security. Until recently, malware,

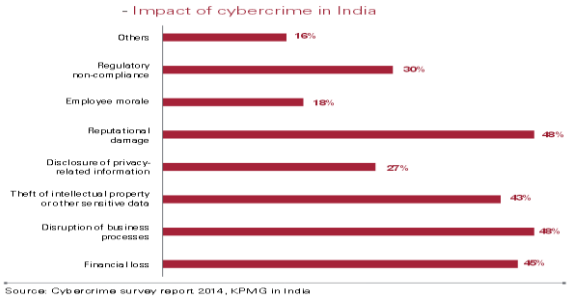
spam emails, hacking into corporate sites and other attacks of this nature were mostly the work of computer 'geniuses' showcasing their talent. These attacks, which were rarely malicious, have gradually evolved into cybercrime syndicates siphoning off money through illegal cyber channels.



The frequency of cyber attacks are increased within one year.

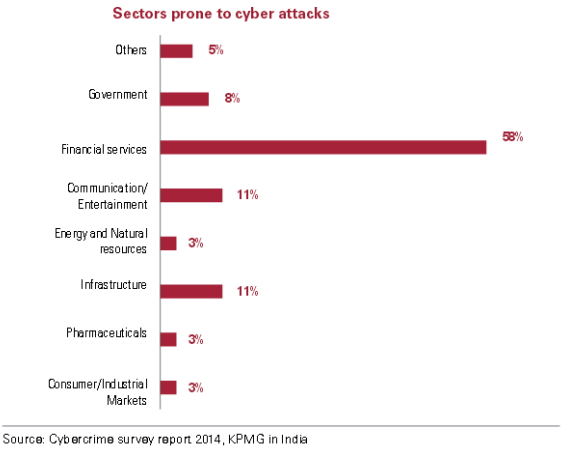
Impact of cybercrime in India

Cybercrime can be developed using various methods; worms are one of the most potent form of cyber attacks that can cause serious disruption in business operations. The Stuxnet computer worm is the first known worm to target and tamper with industrial controls. In September 2010, it infected an unknown number of industrial controls worldwide and could stealthily give false instructions to machinery and false readings to operators. Potentially, it could destroy gas pipelines, cause a nuclear plant to malfunction or cause factory boilers to explode. The worm was known to be most active in Iran, but Indonesia, India and Pakistan also reported infections.



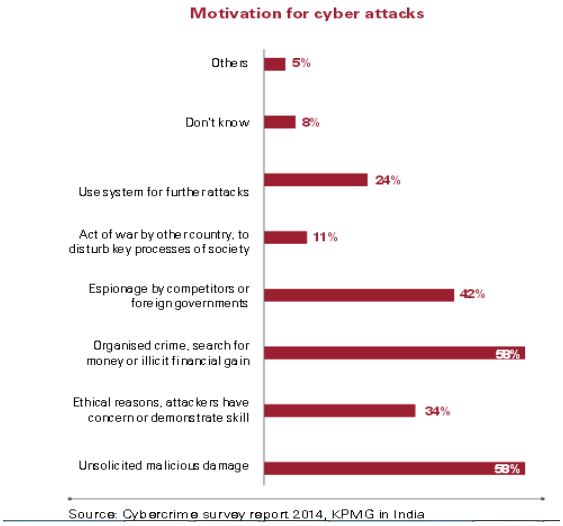
Sectors prone to cyber attacks

In this day and age organisations are extensively using information technology and applications for automation of business processes, also, due to the IT revolution, Internet is now the key medium for business transaction, thereby leaving many sectors vulnerable to cyber attacks. The level of vulnerability of sectors depends on the extent of IT pervasiveness in each of these sectors below, as a result some sectors are more prone to attacks than other sectors.



Motivation for cyber attacks

In the early days, cybercrime attacks were mostly carried out for fun, to demonstrate skills or to achieve one-off financial gains. Nowadays, organised criminals operate with carefully planned and executed attacks not necessarily for the financial rewards, but motivated by activism or digital espionage. These new forms of cybercrime have attention from governments all over the world, since they involve serious risks in the field of disruption of vital functions in society.



Conclusion

This manuscript put its eye not only on the understanding of the cyber crimes but also explains the impacts over the different levels of the society. This will help to the community to secure all the online information critical organizations which are not safe due to such cyber crimes. The understanding of the behavior of cyber criminals and impacts of cyber crimes on society will help to find out the sufficient means to overcome the situation.

The way to overcome these crimes can broadly be classified into three categories: Cyber Laws (referred as Cyber laws), Education and Policy making. All the above ways to handle cyber crimes either are having very less significant work or having nothing in many of the countries. This lack of work requires to improve the existing work or to set new paradigms for controlling the cyber attacks.

References

[1.] Wow Essay (2009), Top Lycos Networks, Available at: http://www.wowessays.com/ dbase/ab2/ nyr90.shtml, Visited: 28/01/2012.

[2.] Bowen, Mace (2009), Computer Crime, Available at: http://www.guru.net/, Visited: 28/01/2012.

[3.] CAPEC (2010), CAPEC-117: Data Interception Attacks, Available at: http://capec.mitre.org/data/definitions/117.html, Visited: 28/01/2012.

[4.] Oracle (2003), Security Overviews, Available at: http://docs.oracle.com/cd/B13789_01/ network.101/ b10777/overview.htm, Visited: 28/01/2012.

[5.] Computer Hope (2012), Data Theft, Available at: http://www.computerhope.com/jargon/d/ datathef.htm, Visited: 28/01/2012.

[6.] DSL Reports (2011), Network Sabotage, Available at: http://www.dslreports.com/forum/r26182468-Network-Sabotage-or-incompetent-managers-trying-to-, Visited: 28/01/2012.

[7.] IMDb (2012), Unauthorized Attacks, Available at: http://www.imdb.com/title/tt0373414/, Visited: 28/01/2012

[8.] Virus Glossary (2006), Virus Dissemination, Available at: http://www.virtualpune.com/citizen-centre/html/cyber_crime_glossary.shtml, Visited: 28/01/2012

[9.] Leagal Info (2009), Crime Overview Aiding And Abetting Or Accessory, Available at: http://www.legalinfo.com/content/criminal-law/crime-overview-aiding-and-abetting-or-accessory. html, Visited: 28/01/2012

[10.] Shantosh Rout (2008), Network Interferences, Available at: http://www.santoshraut.com/ forensic/ cybercrime.htm, Visited: 28/01/2012

[11.] By Jessica Stanicon (2009), Available at: http://www.dynamicbusiness.com/articles/articles-news/one-in-five-victims-of-cybercrime3907.html, Visited: 28/01/2012.

[12.] Prasun Sonwalkar (2009), India emerging as centre for cybercrime: UK study, Available at: http://www.livemint.com/2009/08/20000730/India-emerging-as-centre-for-c.html, Visited: 10/31/09

[13.] India emerging as major cyber crime centre (2009), Available at: http://wegathernews.com/ 203/india-emerging-as-major-cyber-crime-centre/, Visited: 10/31/09

[14.] PTI Contents (2009), India: A major hub for cybercrime, Available at: http://business.rediff.com/ slide-show/2009/aug/20/slide-show-1-india-major-hub-for-cybercrime.htm, Visited: 28/01/2012.

[15.] Crime Desk (2009), Million Online Crimes in the Year: Cyber Crime Squad Established, Available at:http://www.thelondondailynews.com/million-online-crimes-year-cyber-crime-squad-established-p-3117.html, Visited: 28/01/2012.

[16.] Newswise (2009), China Linked to 70 Percent of World's Spam, Says Computer Forensics Expert, Available at: http://www.newswise.com/articles/view/553655/, Visited: 28/01/2012.

[17.] Cyberlawtimes (2009), Available at: http://www.cyberlawtimes.com/forums/index.php?board =52.0, Visited: 10/31/09

[18.] Kevin G. Coleman (2011), Cyber Intelligence: The Huge Economic Impact of Cyber Crime, Available at: http://gov.aol.com/2011/09/19/cyber-intelligence-the-huge-economic-impact-of-cyber-crime/, Visited: 28/01/2012

[19.] Gordon, L. A. et al., 2003, A Framework for Using Insurance for Cyber-Risk Management, Communications of the ACM, 46(3): 81-85.

[20.] D. Ariz. (April 19, 2000), American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc. Civ. 99-185 TUC ACM, 2000 U.S. Dist. Lexis 7299.

[21.] Kelly, B. J., 1999, Preserve, Protect, and Defend, Journal of Business Strategy, 20(5): 22-26.

[22.] Berinato, S. (2002), Enron IT: A take of Excess and Chaos, CIO.com, March 5 http://www.cio.com/executive/edit/030502_enron.html, Visited: 28/01/2012

[23.] Power, R., 2001, 2001 CSI/FBI Computer Crime and Security Survey, Computer Security Issues and Trends, 7(1): 1-18.

[24.] Hoffer, J. A., and D. W. Straub, 1989, The 9 to 5 Underground: Are You Policing Computer Crimes?, Sloan Management Review (Summer 1989): 35-43

[25.] Sprecher, R., and M. Pertl, 1988, Intra-Industry Effects of the MGM Grand Fire, Quarterly Journal of Business and Economics, 27: 96-16.

[26.] Baskerville, R., 1991, Risk Analysis: An Interpretive Feasibility Tool in Justifying Information Systems Security, European Journal of Information Systems, 1(2): 121-130.

[27.] Lyman, J., 2002, In Search of the World's Costliest Computer Virus, http://www. newsfactor.com/perl/story/16407.html. 2002.

ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

[28.] D'Amico, A., 2000, What Does a Computer Security Breach Really Cost?, The Sans Institute

[29.] Hancock, B., 2002, Security Crisis Management—The Basics, Computers & Security, 21(5): 397-401.

[30.] Cyber Trust and Crime Prevention, Mid-Term Review, November 2005 – January 2009, Available at: http://www.bis.gov.uk/assets/bispartners/foresight/docs/cyber/ctcp_midterm_ review.pdf, Visited: 28/01/2012

[31.] Nigel Jones, Director or the Cyber Security Knowledge Transfer Network, was featured in the daily telegraph (May 6, 2008), Cyber Security KTN,

[32.] Nilkund Aseef, Pamela Davis, Manish Mittal, Khaled Sedky, Ahmed Tolba (2005), Cyber-Criminal Activity and Analysis,White Paper, Group 2.

[33.] Stephen Northcutt et al. (2011), Security Predictions 2012 & 2013 - The Emerging Security Threat, Available at: http://www.sans.edu/research/security-laboratory/article/security-predict2011,Visited: 29/01/2012