Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol 2, No.1, 2012

An Overview Study on Cyber crimes in Internet

V.Karamchand Gandhi
Assistant Professor,
Department of Computer Science,
Bharath College of Science and Management,
Thanjavur, Tamil Nadu – South India.
E-Mail: vedhagandhi@gmail.com

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 paper is an attempt to provide a glimpse on cyber crime in India. This paper is based on various reports from news media and news portal.

Keywords: Cyber crime, Hacking, Phishing, Vishing, Cyber squatting

1. Introduction

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. 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 activism, traditional espionage, or information warfare and related activities.

2. 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 behaviour 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 [2].

Cyber stalking is a technologically-based “attack” on one person who has been targeted specifically for that attack for reasons of anger, revenge or control. Cyber stalking can take many forms, including:

- harassment, embarrassment and humiliation of the victim
- emptying bank accounts or other economic control such as ruining the victim's credit score
- harassing family, friends and employers to isolate the victim

The term can also apply to a “traditional” stalker who uses technology to trace and locate their victim and their movements more easily (e.g. using Facebook notifications to know what party they are attending). A true cyber stalker’s intent is to harm their intended victim using the anonymity and untraceable distance of technology. In many situations, the victims never discover the identity of the cyber stalkers who hurt them, despite their lives being completely upended by the perpetrator.

3. 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. 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 [3].

Crackers are people who try to gain unauthorised access to computers. This is normally done through the use of a 'backdoor' program installed on your machine. A lot of crackers also try to gain access to resources through the use of password cracking software, which tries billions of passwords to find the correct one for accessing a computer. Obviously, a good protection from this is to change passwords regularly.

In computer networking, hacking is any technical effort to manipulate the normal behavior of network connections and connected systems. A hacker is any person engaged in hacking [9]. The term "hacking" historically referred to constructive, clever technical work that was not necessarily related to computer systems. Today, however, hacking and hackers are most commonly associated with malicious programming attacks on the Internet and other networks.

M.I.T. engineers in the 1950s and 1960s first popularized the term and concept of hacking. Starting at the model train club and later in the mainframe computer rooms, the so-called "hacks" perpetrated by these hackers were intended to be harmless technical experiments and fun learning activities. Later, outside of M.I.T., others began applying the term to less honorable pursuits. Before the Internet became popular, for example, several hackers in the U.S. experimented with methods to modify telephones for making free long-distance calls over the phone network illegally. As computer networking and the Internet exploded in popularity, data networks became by far the most common target of hackers and hacking.

4. 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 [4].

Phishing is the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user’s information.

For example, 2003 saw the proliferation of a phishing scam in which users received e-mails supposedly from eBay claiming that the user’s account was about to be suspended unless he clicked on the provided link and updated the credit card information that the genuine eBay already had. Because it is relatively simple to make a Web site look like a legitimate organizations site by mimicking the HTML code, the scam counted on people being tricked into thinking they were actually being contacted by eBay and were subsequently going to eBay’s site to update their account information. By spamming large groups of people, the "phisher" counted on the e-mail being read by a percentage of people who actually had listed credit card numbers with eBay legitimately.

Phishing, also referred to as brand spoofing or carding, is a variation on "fishing," the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting [8].

Phishing is an e-mail fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients. Typically, the messages appear to come from well known and trustworthy Web sites. Web sites that are frequently spoofed by phishers include PayPal, eBay, MSN, Yahoo, BestBuy, and America Online. A phishing expedition, like the fishing expedition it's named for, is a speculative venture: the phisher puts the lure hoping to fool at least a few of the prey that encounter the bait. Phishers use a number of different social engineering and e-mail spoofing ploys to try to trick their victims.

5. 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.

Cross-Site Scripting attacks are a type of injection problem, in which malicious scripts are injected into the otherwise benign and trusted web sites [7]. Cross-site scripting (XSS) attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user in the output it generates without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user’s browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by your browser and used with that site. These scripts can even rewrite the content of the HTML page.

6. Vishing

One emerging threat called vishing has already affected thousands of people in the Midwest. In these cases, criminals use the power of Voice over Internet Protocol to spoof caller IDs and prey on unsuspecting financial institution customers. Believing the information displayed on their caller IDs is accurate, customers are willing to share their private personal and financial information with the caller who is not, as their caller ID claims, a financial institution employee [5].

Vishing (voice or VoIP phishing) is an electronic fraud tactic in which individuals are tricked into revealing critical financial or personal information to unauthorized entities. Vishing works like phishing but does not always occur over the Internet and is carried out using voice technology. A vishing attack can be conducted by voice email, VoIP (voice over IP), or landline or cellular telephone.

Vishing is difficult for authorities to trace, particularly when conducted using VoIP. Furthermore, like many legitimate customer services, vishing scams are often outsourced to other countries, which may render sovereign law enforcement powerless.

Consumers can protect themselves by suspecting any unsolicited message that suggests they are targets of illegal activity, no matter what the medium or apparent source. Rather than calling a number given in any unsolicited message, a consumer should directly call the institution named, using a number that is known to be valid, to verify all recent activity and to ensure that the account information has not been tampered with.

8. 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-mai l 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 [6].

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.

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.

9. Conclusion

Net surfing1 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 cyberspace. 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 leave 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.

References

[1] Roderic Broadhurst and Peter Grabosky, “Cyber Crime – The Challenges in Asia”, Hong Kong University Prees, 2005. ISBN: 962-209-724-3.
[2] Paul Bocij, “Cyber Stalking - Harassment in the Internet age and How to protect your family” Library of Congress Cataloging-in-Publication Data, 2004. ISBN:0-275-98118-5.

[3] Jon Erickson, “Hacking – The Art of Exploitation”, William Pollock Publishers, 2nd Edition, 2008. ISBN: 1-59327-144-1
[4] H. Thomas Milhorn, “Cyber Crime – How to Avoid Beconing a Victim”, Universal Publishers, 2007. ISBN: 1-58112-954-8.
[5] Markus Jacobsson and Zulfikar Ramzan, “Crime Ware- Understaning New Attacks and Defenses”, Symantec Press.
[6] Gray Byrne, “Botnets – The Killer Web App”, Syngress Publishing Inc., ISBN: 1-59749-135-7.
[7] Peter Stavroulakis and Mark Stamp, “Handbook of Information and Communication”, Springer. E-ISBN : 978-3-642-04117-4. ISBN: 978-3-642-04116-7.
[8] Mark Stamp, “Information Security – Principles and Practices”, John Wiley & Sons Inc,. ISBN: 978-0-470-62639-9.
[9] Giorgio Franceschetti and Marina Grossi, “Homeland Security – Technology Challenges from sensing and Encrypting to mining and Modeling”, Library of Congress, US. ISBN: 978-59693-289-0.

V.KARAMCHAND GANDHI is currently working as an Assistant professor in the Department of Computer Science, Bharath College of Science and Management, Thanjavur, Tamil Nadu state. He holds his Master’s degree in Computer Science from St.Joseph’s College, Tiruchirppalli. He obtained his M.Phil and MBA degrees to the feather of his educational career. He had six years of experience in teaching and three years of experience in research. He is currently doing research in Wireless networks. He has presented and published more than fifteen research papers in National and International conferences and journals. His research interest includes Computer Networks, Image processing, Compiler design and Digital computer fundamentals. He is life member of various technical societies such as IAENG, IACSIT, etc.