International Journal of Electrical Electronics & Computer Science Engineering
Special Issue - ICSCAAIT-2018 | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

Cyber Crime and Security: A Modern Day Threat

Prashant[1], Abhishek[2], Sonia[3]
[1-2]UG Scholar, School of Computer Science, Lingaya's University, Faridabad, India
[3]Assistant Professor, School of Computer Science, Lingaya's University, Faridabad, India

Abstract: ***This paper gives a brief insight to one of the trending topics around i.e. Cyber crimes and security. It presents various illicit activities such as forgery, cyber stalking and bullying, unauthorize access to systems, phishing, DDOS, creating and spreading malwares, Cyberterrorism, Spam etc that is taking place over internet and violating our fundamental rights. It contains specific computer crimes, documented cases, applicable laws, security, approaches and some preventive measures to avoid being victim of any nefarious designs. The primary objective is to aware reader about modern day crimes by updating you with the approaches and methods to be undertaken.***

Keywords: Cybercrime, Malwares, DDOS, Phishing, Cyber Stalking, Spam Cyber Terrorism

I. INTRODUCTION

The terms computer crime and cybercrime are more properly restricted to describing criminal activity in which the computer or network is a necessary part of the crime, these terms are also sometimes used to include traditional crimes, such as fraud, theft, blackmail, forgery, and embezzlement, in which computers or networks are used. As the use of computers has grown, computer crime has become more important.

Computer crime can broadly be defined as criminal activity involving an information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), and electronic fraud.

Computer crime issues have become high-profile, particularly those surrounding hacking, copyright infringement through warez, child pornography, and child grooming. There are also problem of privacy when confidential information is lost or intercepted, lawfully or otherwise.

II. SPECIFICE COMPUTER CRIMES

Malware: Malware is Malicious Software - deliberately created and specifically designed to damage, disrupt or destroy network services, computer data and software.

There are several types of computer virus program which can copy itself and surreptitiously infect another computer, often via shared media such as a floppy disk, CD, thumb drive, shared directory, etc. Viruses are always embedded within another file or program.

Worm: self-reproducing program which propagates via the network.

Trojan Horse: program which purports to do one thing, but secretly does something else; example: free screen saver which installs a backdoor

Root Kit: set of programs designed to allow an adversary to surreptitiously gain full control of a targeted system while avoiding detection and resisting removal, with the emphasis being on evading detection and removal

Botnet: set of compromised computers ("bots" or "zombies") under the unified command and control of a "botmaster;" commands are sent to bots via a command and control channel (bot commands are often transmitted via IRC, Internet Relay Chat).

Spyware: assorted privacy-invading/browser-perverting programs

Malware: an inclusive term for all of the above -- "malicious software

Ex: David Smith & The Melissa Virus Example

Spam: Spam, or the unsolicited sending of bulk email for commercial purposes, is unlawful to varying degrees. As applied to email, specific anti-spam laws are relatively new, however limits on unsolicited electronic communications have existed in some forms for some time.Spam originating in India accounted for one percent of all spam originating in the top 25 spam-producing countries making India the eighteenth ranked country worldwide for originating spam.

Phishing: Phishing is a technique used by strangers to "fish" for information about you, information that you would not normally disclose to a stranger, such as your bank account number, PIN, and other personal identifiers such as your National Insurance number.

Fraud: Computer fraud is any dishonest misrepresentation of fact intended to induce another to do or refrain from doing something which causes loss. In this context, the fraud will result in obtaining a benefit by:

1. Altering computer input in an unauthorized way.
2. Altering or deleting stored data; or

3. Altering or misusing existing system tools or software packages, or altering or writing code for fraudulent purposes.

Other forms of fraud may be facilitated using computer systems, including bank fraud, identity theft, extortion, and theft of classified information (Csonka, 2000)

1. Obscene Or Offensive Content: The content of websites and other electronic communications may be distasteful, obscene or offensive for a variety of reasons. In some instances, these communications may be illegal.

2. Harassment: Whereas content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing for example on gender, race, religion, nationality, sexual orientation. This often occurs in chat rooms, through newsgroups, and by sending hate e-mail to interested parties (see cyber bullying, cyber stalking, harassment by computer, hate crime, Online predator, and stalking). Any comment that may be found derogatory or offensive is considered harassment.

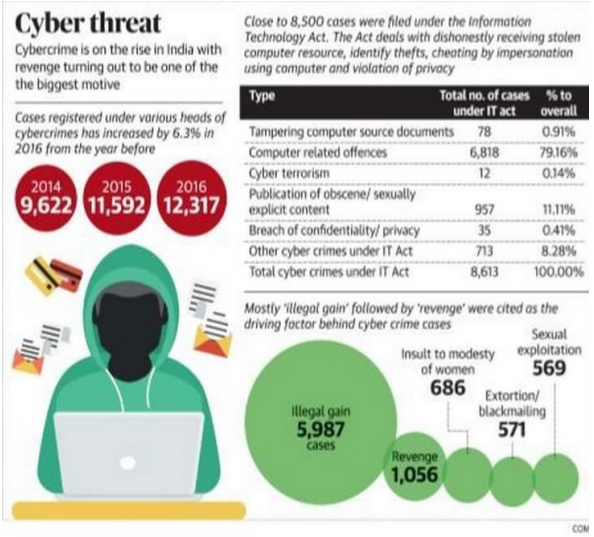
3. Drug Trafficking: Drug traffickers are increasingly taking advantage of the Internet to sell their illegal substances through encrypted e-mail and other Internet Technology. Some drug traffickers arrange deals at internet cafes, use courier Web sites to track illegal packages of pills, and swap recipes for amphetamines in restricted-access chat rooms. The rise in Internet drug trades could also be attributed to the lack of face-to-face communication. These virtual exchanges allow more intimidated individuals to more comfortably purchase illegal drugs. The sketchy effects that are often associated with drug trades are severely minimized and the filtering process that comes with physical interaction fades away. Furthermore, traditional drug recipes were carefully kept secrets. But with modern computer technology, this information is now being made available to anyone with computer access.

4. Cyber Terrorism: Cyber terrorism in general, can be defined as an act of terrorism committed through the use of cyberspace or computer resources (Parker 1983). As such, a simple propaganda in the Internet, that there will be bomb attacks during the holidays can be considered cyberterrorism. At worst, cyberterrorists may use the Internet or computer resources to carry out an actual attack. As well there are also hacking activities directed towards individuals, families, organised by groups within networks, tending to cause fear among people, demonstrate power, collecting information relevant for ruining peoples' lives, robberies, blackmailing etc.

III. DOCUMENT CASES

- In late 2015, JP and Morgan Chase & Co. target of giant hacking conglomerate, where financial related data extracted and exposed globally.
- On 17 Feb 2017, Cloudfare announced that a bug in its platform caused random leakage of potentially sensitive customer data.
- On 19 June 2017, 198 million voter records exposed that were hosted on an Amazon S3 server.
- On 16 May 2017 strain of ransomware called WannaCry spread around the world, encrypting thousands of computers around the world, demanding ransom to restore affected systems.
- On 7 Dec. 2017, Cyberthieves loot tens of millions in bitcoin NiceHash cryptocurrency marketplace
- On 15 Dec. 2017, Attacker exploit old WordPress to inject sites with code enabling redirection, takeover.

In India, National Crime Records Bureau (NCRB) has shared information graph related to cyber crimes that took place recently. This shows how vulnerable are we as a user, how securely we are using internet. A country of million of users are in persistent threat of the technology and they are being targeted for their poor knowledge of cyber security. The illustration displays cases that have been reported but what about those which go unreported. We need to pay attention while working on internet and keep ourselves updated with upcoming threats.



IV. APPLICABLE LAW IN INDIA

With the emergence of technology the misuse of technology has also expanded to its optimum level and then there arises a need of strict statutory laws to regulate the criminal activities in the cyber world and to protect technological advancement system. It is under these circumstances Indian parliament passed its "Information Technology Act, 2000" on 17th oct to have its exhaustive law to deal with the technology in the field of e-commerce, e-governance, e-banking as well as penalties and punishments in the field of cybercrimes.

- Cyber Crime against persons like cyber-stalking, defamation, spreading obscene material, harassment, card cloning, cheating and fraud, assault by threat, SMS spoofing, E-mail spoofing.
- Crime Against Persons Property like Intellectual property crimes, Cyber squatting, Cyber vandalism. Transmitting virus, cyber trespass, internet time thefts.
- Cybercrimes Against Government like Cyber warfare, distribution of pirated software, possession of unauthorized information.
- Cybercrimes Against Society at large like Child pornography, Cyber Trafficking, Online Gambling, Financial Crimes, Forgery.

Penalty For Damage To Computer System: According to the Section: 43 of 'Information Technology Act, 2000' whoever does any act ofdestroys, deletes, alters and disrupts or causes disruption of any computer with the intention of damaging of the whole data of the computer system without the permission of the owner of the computer, shall be liable to pay fine upto 1crore to the person so affected by way of remedy. According to the Section:43A which is inserted by 'Information Technology(Amendment) Act, 2008' where a body corporate is maintaining and protecting the data of the persons as provided by the central government, if there is any negligent act or failure in protecting the data/ information then a body corporate shall be liable to pay compensation to person so affected. And Section 66 deals with 'hacking with computer system' and provides for imprisonment up to 3 years or fine, which may extend up to 2 years or both.

V. CRIME SECURITY

Computer security is a branch of technology known as information security as applied to computers and networks. The objective of computer security includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users.

Some Approaches:

Here are several approaches to security in computing, sometimes a combination of approaches is valid:

1. Trust all the software to abide by a security policy but the software is not trustworthy (this is computer insecurity).
2. Trust all the software to abide by a security policy and the software is validated as trustworthy (by tedious branch and path analysis for example).
3. Trust no software but enforce a security policy with mechanisms that are not trustworthy (again this is computer insecurity).
4. Trust no software but enforce a security policy with trustworthy mechanisms.

Hardware Mechanisms that Protect Computers and Data:

Hardware based or assisted computer security offers an alternative to software-only computer security. Devices such as dongles may be considered more secure due to the physical access required in order to be compromised.

While many software based security solutions encrypt the data to prevent data from being stolen, a malicious program may corrupt the data in order to make it unrecoverable or unusable. Hardware-based security solutions can prevent read and write access to data and hence offers very strong protection against tampering.

Secure Operating Systems:

One use of the term computer security refers to technology to implement a secure operating system. Much of this technology is based on science developed in the 1980s and used to produce what may be some of the most impenetrable operating systems ever. Though still valid, the technology is in limited use today, primarily because it imposes some changes to system management and also because it is not widely understood. Such ultra-strong secure operating systems are based on operating system kernel technology that can guarantee that certain security policies are absolutely enforced in an operating environment. An example of such a Computer security policy is the Bell-La Padula model. The strategy is based on a coupling of special microprocessor hardware features, often involving the memory management unit, to a special correctly implemented operating system kernel. This forms the foundation for a secure operating system which, if certain critical parts are designed and implemented correctly, can ensure the absolute impossibility of penetration by hostile elements. Ordinary operating systems, on the other hand, lack the features that assure this maximal level of security. The design methodology to produce such secure systems is precise, deterministic and logical.

If the operating environment is not based on a secure operating system capable of maintaining a domain for its own execution, and capable of protecting application code from malicious subversion, and capable of protecting the system from subverted code, then high degrees of security are understandably not possible. While such secure operating systems are possible and have been implemented, most commercial systems fall in a 'low security' category because they rely on features not supported by secure operating systems (like portability, et al.). In low security operating

environments, applications must be relied on to participate in their own protection. There are 'best effort' secure coding practices that can be followed to make an application more resistant to malicious subversion.

In commercial environments, the majority of software subversion vulnerabilities result from a few known kinds of coding defects. Common software defects include buffer overflows, format string vulnerabilities, integer overflow, and code/command injection.

Some common languages such as C and C++ are vulnerable to all of these defects (see Seacod, *"Secure Coding in C and C++"*). Other languages, such as Java, are more resistant to some of these defects, but are still prone to code/command injection and other software defects which facilitate subversion.

In summary, 'secure coding' can provide significant payback in low security operating environments, and therefore worth the effort. Still there is no known way to provide a reliable degree of subversion resistance with any degree or combination of 'secure coding.'

VI. CONCLUSION

Computer security is critical in almost any technology-driven industry which operates on computer systems. Computer security can also be referred to as computer safety. The issues of computer based systems and addressing their countless vulnerabilities are an integral part of maintaining an operational industry.

VII. REFERENCES

[1] Cybersecurity and Cyberwar: What everyone Needs to Know? By Allan Freidman and P.W. Singer.

[2] Morrie Gasser: Building a secure system, ISBN 0-442-23022-2 1988.

[3] The Art of Deception 2001: Kevin Mitnick and William L. Simon.

[4] E. Stewart Lee: Essays about Computer Security Cambridge, 1999.

[5] Paul A. Karger, Roger R. Schell: Thirty Years Later: Lessons from the Multics Security Evaluation, IBM white paper.

[6] Bruce Schneier: Secrets & Lies: Digital Security in a Netwoked World, ISBN 0-471-25311.