MEDWIN PUBLISHERS
Committed to create value for Researchers

International Journal of Forensic Sciences
ISSN: 2573-1734

Examination of Cyber Crime in Special Reference of Non- Technical Attacks

Sarawagi K* and Srivastava A

Dr. APJ Abdul Kalam Institute of Forensic Science & Criminology, Bundelkhand University, India

Conceptual Papers

Volume 2 Issue 1

Received Date: January 29, 2017

Published Date: April 05, 2017

***Corresponding author:** Sarawagi K, Dr. APJ Abdul Kalam Institute of Forensic Science & Criminology, Bundelkhand University, India, E-mail: mailme.ketansarawagi@gmail.com

Abstract

Cyber Forensics is a challenging and rapidly growing field of forensic Science. It involves collection and examination of electronic evidence. It appraises the damage to a computer or any network as a result of any electronic attack. It also recovers the lost informational data from such a system to chase a threat. The cyber attacks mainly are of two types: Technical Attacks and Non-Technical attacks. Technical attacks are those which were introduced by programming and coding. Whereas Non-technical attacks are those which can be attempted with the help of software and predefined programs.

Nowadays most of the non technical attacks are being attempted by the young generation without knowing the consequences of such attacks. This paper seeks to introduce the fundamental technologies including tools and techniques used in commission of above discussed types of cyber attacks and it's forensic analysis. Topics covered include type of non technical attacks, causes, technology of key logging software and devices technology. This also covers the phishing attacks, use of some spying software like Trojan, sniffer, and the legal and ethical aspects of computer forensics to combat and investigate such crimes. This paper serves as a conceptual study for introduction into the extensive and intricate area known as computer forensics that could be useful for investigative and law enforcement agencies.

Keywords: Computer crime; Internet fraud; Computer hackers; Government secrecy; Identity theft; False impersonation; Globalization; Social media; Technical attacks; Non-technical attacks; Phishing; Key logging

Introduction

Without any doubt in this era globalization with science and technology is playing a vital role in the development of the human society. Thus, it is making human life more comfortable and sophisticated. Forwarding in its path APRANET the predecessor of internet in the field of information technology was introduced and now a days internet has became one of the basic need of any individual [1]. In 1980s the

emergence of internet has given birth to the cyber space and in these last two decades use of internet has increased exponentially and this has been resulted in genesis of the 'Cyber Crime' [2].

Cyber crime can be classified according to the different factors, considering the classification according to the way they are attempted they can be classified into two categories that are as follows:

- Technical
- Non Technical

Technical Cyber Attacks

Technical Cyber crimes are those cyber crimes in which the offender uses his/her technical knowledge while attempting the threat. Technical knowledge means the knowledge about the hardware, software, and its development by high level languages.

Non Technical Cyber Attacks

Non technical attacks are those attacks in which the attacker uses some specified software and technique and by following some simple steps the offender commits threats. There is no need of any technical knowledge to perform these threats.

Nowadays the youngsters are attempting the Non-technical attacks very frequently without knowing the consequences of the same. Here the questions raises what are the factors which makes the delinquents to attempt any crime?

Causes of increasing frequency of attempts of Non Technical Cyber Attacks

- Tendency to prove themselves more intelligent among their fellows.
- Testing their skills
- Fever of term HACKING
- Online competitions of hacking (Challenges).
- Easy available online tutorials of hacking.
- Easy availability of pirated software.
- Monetary gain.
- Seduction.
- Exterior pressure (Daunt, appal,)

Some of the Non Technical Attacks have been discussed bellow

Key loggers Attacks

In these attacks a software called key logger is used which logs each and every keystrokes on the keyboard by the victim. Then either saves them on a text file or send them to the offender's mail inbox once after a defined time period by the attacker [3,4]. Key loggers usually are small programs and that's why they consumes slight disk space and can appear as utility software, thus it is very hard to detect.

DOS / DDOS Attacks

These attacks involve flooding any computer resource or one can say server of any network by sending lots of requests than it can handle. This results in denying of services offered by the resource to the authorized users due to system crash. In these threats the target machine is saturated from the external requests by increasing the traffic in the network, such that it becomes unable to respond such a heavy traffic, or responds much slowly as to be rendered effectively unavailable. DoS attacks are generally implemented by:

1. Slamming the targeted computer(s) to reset, or consume its resources such that it becomes unable to provide its intended service.
2. Obstructing the communication media used between the intended user and the target so that their communication gets interrupted.

Another type of denial of service attack is Distributed Denial of Service (DDoS) attack wherein many offenders geographically dispersed are involved. It is very difficult to counter strike such an attack. The attack is initiated by sending excessive requests (eco request) to the victim's computer(s) and when the limit that the victim's server can support exceeded thereby it results as server crash [5].

Sniffing Attacks

Across the Internet any type of data travels in the form of individual packets, in variable size, that are called as "data packets". Since the users never pay attention to any of this raw data, without their knowledge many spyware systems by stealth send their sensitive information out of their computer system. Packet sniffing is a method of

excitation of each packet as it flows across the network [6]; in this technique attacker sniffs data belonging to the victims communicating on the network. It depends on the user of the Packet sniffers software it can be used for the administrative purpose or as a tool to perform a threat. Network sniffers can capture sensitive part of information passing through the network as well as passwords of the victim.

Trojan Attacks

As such to the wooden horse, a Computer Trojan Horse program contains some hidden inimical functionality which is wrapped as a program that appears to have some useful or benign purpose [7]. By employing like-minded trickery Trojan horses try to bypass the computer security barricades (such as firewalls). By wrapping like any normal software, Trojan horse programs are exercised for the following objectives:

• Making a user to install the Trojan horse in to the computer system. In this way, by the Trojan horse Attacker gets an opened back door for the entry of the malicious software on to the computer system.

• By looking as the "normal" programs running on a computer system, the Trojan horse hide itself from the users and administrators so that they continue their activities, unaware of the malicious activity going on their system. There are lots of methods to hide the malicious capabilities of any wares on computer system of the user.

In this way we should keep in our mind that the attackers have a main aim to hide the malicious code so that the victims could not realize the malicious activity by the offender.

Detection of Non- Technical Attacks

- Forensic examination of Registry of Operating System.
- Analysis of Services Activated on computer system.
- Analysis of the cookies found while data retrieving by FTK, Oxygen Forensic, cellebrite, Encase and much more.
- Examination of the header, footer and client IP address of the e-mail or other data packet.
- Monitoring the flow of the data packet into the network.

Conclusion

As per the above discussion it can be concluded that science and technology is like fire flame thorough which we can prepare our food or burn our hand, similarly use of internet in one hand playing a very important role in globalization and Information technology but on other hand over use of Internet has given birth to cyber space which is acting as a platform for the cyber threats.

In this age of digitalization, where the Internet in field of information and technology has become a very important part, users of internet and governments are facing an increased risk to become the targets of cyber crimes. The attackers are continuously developing and advancing their techniques with the advancement in technology; they are also reshuffling their targets — focusing less on retrieving of financial information and more on business espionage and accessing confidential information related to the government. Governments must cooperate globally to develop an effective model that will counter strike and the control the threat and also helpful to combat against the fast-spreading cyber crime.

But precaution is better than cure in this way some protection tips are given bellow:

- 'Auto update' option for your browser and plug-ins should be Turned on.
- Use an Anti- malware.
- Anti-malwares by different brands can be use for extra security.
- For your FTP set a strong password.
- Check the configuration of FTP client settings timely. Use of SFTP is more secured.
- To secure your communication with others Use VPN.
- Use a firewall.
- Use WPA2 for your wireless connections.
- Configure your browser settings to prevent DOS/DDOS attacks by changing the request limits and also observing the maximum connections per server.
- Turn on Firewall protection.
- Use a suitable antivirus and update it properly.

References

1. Tiwari RK, Sastry PK, Ravi Kumar KV (2002) 'Computer crime and computer forensic', first edition, select publishers, Pandav nagar Delhi.

2. Schell H (2004) dernadette and Martin Clemens, Cyber crime (A reference handbook), ABC-CLIO, Inc. santa borbura California 1(4): 220.

3. Stephension peter (1999) Investigating Computer related crime first edition, CRC press BocaRaton London, Newyork Washington DC, Pp: 82-83.

4. Singh YK (2005) Cyber crime and law first edition, Shree publisher and distributers 20 Ansari road dariya ganj New Delhi.

5. Mishra RC (2005) Cyber crime impact in the new millenniums first PB edition, Authors press Laxmi nagar New Delhi.

6. (2003) Issues in Computer Forensics Bui Sonia, Enyeart Michelle, Luong Jenghuei COEN 150 Dr. Holliday.

7. Emmett Paize Jr (1996) The future of information technology.