ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 1, January 2018

Survey On Cyber-Crime Attacks and its Techniques

S.Asha[1], C.Bala Krishnan[2]
M.E Student[1], Associate Professor[2]
S.A Engineering College, Chennai, India
ashaarun1220@gmail.com[1],balakrishnan@saec.ac.in[2]

Abstract:

Cyber-crime is the crime committed either using the internet or the computers in order to steal the person’s identity or to perform the illegal imports. In Cyber-crime computers are used as an object in order to perform the crime by the attackers. Cyber-Crime is also termed as Computer Crime.In cyber-crimes, computers are used as a tool to commit fraud. In this paper, we summarize about the cyber-crimes, its types and techniques to avoid these crimes.

Keywords:cyber-crime, cyber criminals, cyber security, cyber law.

I. Introduction:

The first cyber-crime activity occurred in the year 1820. Cyber-crime is the crime committed either using the internet or the computers in order to steal the person’s identity or to perform the illegal imports. In Cyber-crime computers are used as an object in order to perform the crime by the attackers. Cyber-Crime is also termed as Computer Crime. In cyber-crimes, computers are used as a tool to commit fraud. In this paper, we summarize about the cyber-crimes, its types and steps to avoid these crimes

In 21st century it is necessary for every individual to know about the effects of cyber-crime activities, since we are using the internet for carrying out most of theactivities such as online transactions, credit card payments etc.,

2. Cyber criminals:

Cyber criminals are the individuals or the group of individuals who perform cyber-crime using the computers. They are also known as hackers, hijackers, attackers, hacktivists etc. There are two types of attacks performed by these attackers using computers.

They are

1. Computer as a target
2. Computer as a weapon

Computer as a target:

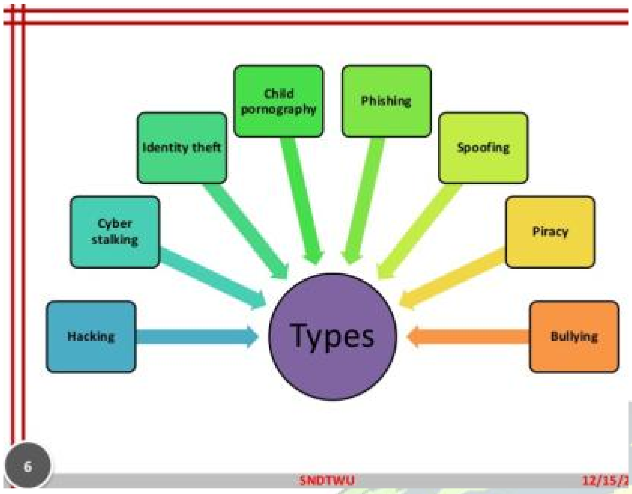
In this attack, attackers use computer as a target inorder to attack other computers. Example for these attacks are hacking, virus/worm attacks and DOS attacks.

Computer as a weapon:

In this attack, computers are used as a weapon or a tool in order to perform real world crimes. Some examples for these attacks are cyber terrorism, credit card frauds, child pornography etc.

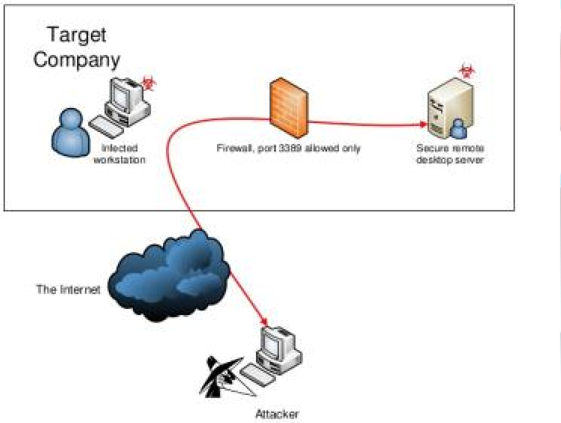
3. Types of Cyber Crime:

Cyber-crime attack comes in different shapes and forms. The reason for cyber-crime attack also varies. There are different types of cyber-crimes attack. They are



Hacking:

Hacking is also termed as hijacking. Hacking is nothing but gaining unauthorized access to the computer or the networks in a system. An individual who perform the hacking activities are referred as the hackers. Hackers may alter the system or change the security features of the network in order to accomplish the task which is different from the original task of the system.

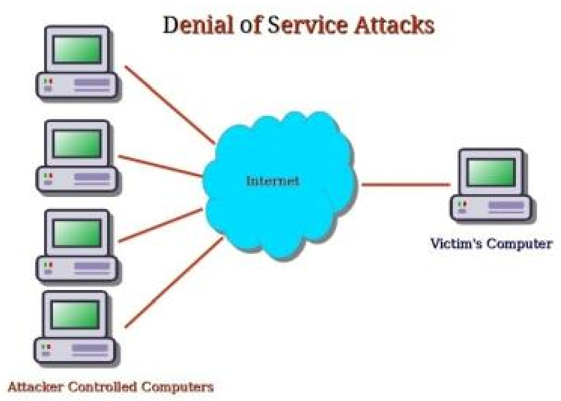

Target Company
Infected workstation
Firewall, port 3389 allowed only
Secure remote desktop server
The Internet
Attacker

Hackers use several techniques for hacking the system and they are `

- Vulnerability Scanner
- Password cracking
- Packet Sniffer
- Spoofing Attack
- Trojan horse
- Viruses
- Key loggers

Denial-of-service:

Denial-of-service attack also known as DOS attack is a type of attack in which the legitimate users are prevented from accessing the system or a network. In this attack, the internet server of the victim is over flooded with the continuous request making the server to crash and becomes unavailable for the use by intended user. [4] discussed about a method, Wireless sensor networks utilize large numbers of wireless sensor nodes to collect information from their sensing terrain. Wireless sensor nodes are battery-powered devices. Energy saving is always crucial to the lifetime of a wireless sensor network. Recently, many algorithms are proposed to tackle the energy saving problem in wireless sensor networks. There are strong needs to develop wireless sensor networks algorithms with optimization priorities biased to aspects besides energy saving. In this project, a delay-aware data collection network structure for wireless sensor networks is proposed based on Multi hop Cluster Network. The objective of the proposed network structure is to determine delays in the data collection processes. The path with minimized delay through which the data can be transmitted from source to destination is also determined. AODV protocol is used to route the data packets from the source to destination.



Virus:

Virus is a malware that gets duplicated and attaches itself to the host system. Virus when executed, it gets replicated and attaches itself to the host system and causes damages to the system. The antivirus software is used to protect the system from the virus attack. There are different types of virus available that may cause damage to the system and they are

1. Email Virus
2. Boot Sector Virus
3. Resident Virus
4. Polymorphic Virus
5. Multipartite Virus
6. File Infector Virus
7. Macro Virus

Software Piracy:

Software piracy is referred to as an illegal replication and distribution of software. Software piracy occurs when several copies of the software are installed into the personal computers or the work computers.

There are four different types of software piracy. They are

- Internet Piracy
- End User Piracy
- Client-Server Overuse
- Hard-Disk Loading

Credit card Fraud:

Credit Card fraud occurs when the card is stolen or lost or when information from the card such as the card details and corresponding pin are stolen. Attackers use these information either to buy goods in the name of the legitimate user or to transfer money from the legitimate user account. Credit card fraud most often occurs through the phishing attacks.

Ransomware:

Ransomware is a type of malicious software that blocks the access to the user system or the files until the ransom is made.Once the payment is done the attackers will allow the users to access their system or the files.

Phishing attack:

Phishing attack is a type of attack which is often carried out in order to steal the data from the user such as login credentials and the credit card number details. In this attack, the attackers disguise themselves as an trusted entity in order to obtain the username, password and the card details to perform a transaction using these details.

4. Safety tips to avoid cyber-crime attacks:

The following steps are used to avoid cyber-crime activities.

- Awareness about cyber-crime activities is essential.
- Install anit-virus software, firewalls, spam blocking software in our personal computers and work computers.
- Identify secure websites while performing online transactions.
- Don’t open or act to the emails sent from an unknown individual.

- Carefully read the privacy policy before submitting data through the internet.

- Unnecessary software must be uninstalled from the computers.
- It is always necessary to check the security settings often.
- Disable the remote connectivity.
- Learn more about the internet policy.

5. Cyber Security:

Cyber Security also known as internet security is a branch of computer security related to the internet. Its objective is to establish guidelines and actions in order to avoid cyber-crime attacks that occurs over the internet.

6. Techniques used by cyber-security:

Cyber security has achieved its goal in reducing the number of unauthorized access of data by the attackers. The techniques that are used to handle the cyber security concerns are

- Authentication
- Encryption
- Digital signature
- Anti-Virus
- Firewall

II. Related Work

A. Understanding of Cyber-Crime attacks:

Cyber-crime is the crime that has been committed either using the internet or the computers in order to steal the person's identity or to perform the illegal imports. In addition to this, it is necessary to know the different kinds of cyber-crimes that occurs all over the world and their preventive measures. According to National Incident-Based Reporting System (NIBRS), cyber-crimes can be classified as crime against society, property and crime against person.

B. **Cyber Crime Information System for Cyber-ethics Awareness:**

Cyber-crimes that include hacking, password trafficking, violation of copyrights, online pornography, Denial of Services (DOS) attacks and any other crimes committed using a computer network should be consideredand actions against them has to be taken. Micro level and macro level Cyber-crime database services should be created. These database services have to attract public in order to utilize the services of portal by increasing awareness about cyber security and availability effective services.

C. Cyber security Principles for Industry and Government:

There are five principles or techniques available in order to improve the cyber security. In order to have continued viability of the infrastructure and growth of their sector, technology companies are highly motivated to design and build security of their products and systems. For economic growth and protection the governments need to secure global information infrastructure. It is required to enhance cyber security at a global level and efforts should be taken on that line. Risk management should be considered to avoid security breaches and crimes.

D. **Cyber Crime Control in Developing Countries' Cyber Cafes:**

Developing countries are more vulnerability to Cyber-crime attacks. These countries lack major infrastructural devices for controlling the Cyber-crimes. Cyber-crime rates are high in developing countries. In order to control the crime rate in developing countries, cyber-crime laws that have been enacted to control and tackle the problem of Cyber-crimes. U.S. is leading in the area of Cyber-crime laws, the European Union countries are next to the industrialized countries in the subject of Cyber-crime law's enactment. There is a gap that exists between the developed countries and the developing countries in the subject of Cyber-crime control and security which must be bridged immediately. The developing countries should unite with the governments of the developed countries to bridge the gap by following the guidelines that have been laid down by theG8 countries and the European Union. The final goal should be to make sure every country in the world should participate in the Cyber-crime control and in the electronic community.

E. **National Cyber Security Policy:**

The Department of Information Technology has proposed a draft for National Cyber Security Policy for secure computing environment and adequate trust & confidence in electronic transactions which has focused on Security of cyber space, enabling the Process, Enabling technologies – Deployment and R&D, Enabling people and Responsible actions by user community. These factors consider information gathering from multiple sources and monitoring of real time assets that need protection and adequate expertise and process to deal with crisis management. For this trained and qualified manpower along with suitable incentives are required.

F. Framework for Improving Critical Infrastructure Cyber security:

The framework for cyber security used by US government is given. The framework was created in collaboration with private sector which use common language to address and manage cyber security risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses. The framework guides cyber security activities for business. It consists of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The Framework helps organizations to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. The Framework provides the organization to structure today's cyber security problems by following standards, guidelines, and practices that are working effectively in industry today.

III.Conclusion

The cyber-crime is a new-fangledinnovation of crimes made by a class of intelligent and well-trained criminals. Earlier these crime occurred in different forms and the criminal law was almost unaware of such types of crimes Cyber-crimesbegan to work when innovation achieves its pinnacle and took new tum to fulfill human needs and requirements. In order to prevent cyber-crimes, user must be aware about the dangers of advanced malware which are taking place nowadays. Cyber-crime laws that have been enacted in order to control and tackle the problem of Cyber-crimes. Government should take serious actions on the individual who involve in the cyber-crime attacks.

References

[1]. A.B. Patki , S. Lakshminarayanan, S. Sivasubramanian& S.S. Sarma published in their paper on — "Cyber Crime Information System for Cyber-ethics Awareness".

[2]. Alex Roney Mathew, Aayad Al Hajj & Khalil Al Ruqeishi has published in their paper —"Cyber Crimes: Threats and Protection".

[3]. Ravi Sharma, "Study of Latest Emerging Trends on Cyber Security and its challenges to Society", International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1 ISSN 2229-5518 IJSER © 2012.

[4] Christo Ananth, T.Rashmi Anns, R.K.Shunmuga Priya, K.Mala, "Delay-Aware Data Collection Network Structure For WSN", International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Volume 1,Special Issue 2 - November 2015, pp.17-21

[5] Loren Paul Rees, Jason K. Deane , Terry R. Rakes , Wade H. Baker, Decision support for Cyber security risk planning, Department of Business Information Technology, Pamplin College of Business, Virginia Tech., Blacksburg, VA 24061, United States b Verizon Business Security Solutions, Ashburn, VA 20147, United States.