Recent Trends in Cyber Crime and Challenges in preventing Cyber Crimes

Dr. M. Umadevi
Professor, Universal College of Engineering and Technology

Abstract **- Recent advances in technology have led to the tremendous increase in digital data. The digital devices are playing vital role in day-to-day transactions. Usage of digital devices leads to more digitization of data like personal information, bank account details, password etc. Hence the security of digital data and transferring data securely has become more important. This confidential data is accessed by individual by attacking the target system or target network. Attackers are exploiting vulnerabilities in the technologies to achieve their goals. This paper explains cybercrime categories and different preventive measure to safeguard sensitive information from attacks.**

I.INTRODUCTION

In today's digital age the use of computers, laptops, tablets and smart phones has become very common. Most of the people dependent on technology to complete their regular tasks through network like sending documents through email, make phone calls through wireless devices, sharing pictures through Facebook, Instagram and Snapchat, and connect with the world through Twitter and LinkedIn.

Internet is the largest communication and information exchange medium now and it is used for development of business, education etc., At the same time Internet is becoming an instrument of numerous types of cyber crimes. It is being used to steal and manipulate the information of users. Important data is being stolen and personal as well as organizational threats are being imposed upon the users which are using Internet. Sensitive information, secret credentials and even the bank account details are being stolen these days with the use of Internet. The Internet space or cyber space is growing very fast and as the cyber crimes.

Cyber-attack is defined as "the exploitation of cyberspace for the purpose of accessing unauthorised or secure information, spying, disabling of networks and stealing both data and money" [1].

Cyber crime is a crime that involves digital devices like computer and network. Digitization of data involves security of data like managing passwords, confidentiality of OTP. As with technology the top cyber crimes defined as

- loss or damage to computer source transmission in electronic form
- hacking
- Tampering of digital data
- Breach of confidentiality

The nature of cyber crime has transformed by the computer use and ICT based tool by extending it to financial transaction, sexual offending, harassment and threshold behaviour and commercial damage. in [2]

- Cyber dependent crime are the offences that committed by using a computer, network or ICT. It involves spread of viruses and other malicious software. They primarily act s directed against computer.
- Cyber enabled crime are increased in their scale and they can reach with or with out ICT like phishing of emails, theft of personal information
- Some reasons in increase in number crimes are listed below
- Easy money without revealing the identity because they use hacked computers and fake or stolen I.P. Address.
- The complex technologies and coding increase the chances of error which the criminals take advantage of.
- Evidence in the form of data can be easily destroyed
- Cyber security is becoming a serious issue for the complete world with intruders attacking people or organizations with the motive of getting access to their restricted content.

II. COMPUTER INTRUSION

There are different methods used to compromise computer system. This varies based on nature of target information system or network and skills of attacker. In [3] computer intrusion described in four phases.

Reconnaissance: Process of obtaining information on target organization or individual to compromise the target.

Attack: Process of applying a technique to compromise target which results in unauthorized access or denial of service

Entrenchment: This is process of continued hidden administrative access to target system

Abuse: Process of conducting further activities on compromised targets to achieve goals of attacker

In computer intrusion the attacker leaves traces of their presence through the environment file system, registry, system logs.

Intrusion detection systems is software or device designed to monitor system or network for the malicious activities or violation of security policies. Intrusion detection systems are categorized as Host Based Intrusion detection (HIDS)and Network Based intrusion detection system(NIDS). IDS with capabilities of response to intrusion is called Intrusion prevention systems. These Intrusion Prevention systems submit reports to system administrator to take necessary preventive action like configuration of firewall to avoid future attacks.

III. TYPES OF CYBER CRIME

Various categories of cybercrimes and safeguards to overcome those cybercrimes are discussed in this section

Malware: These attacks include spyware and remote administration malware, provides login credentials, sensitive business data, or information on the system to attacker. The third most popular kind of malware attack is the dreaded ransom ware, which typically locks your device or takes your data hostage until you pay the hacker to release it. These attacks can be prevented by using latest versions of operating systems.

Few techniques to prevent attacks of ransom ware is patch management of software, frequent backup of data , layered security approach and use of advanced generation fire walls

Phishing is fraudulent attempt to get sensitive information from target people or institution by masquerading as trusted entity. In phishing attack fraudsters earn huge amount of money by misleading the victim by acting as a bank manager where they ask for sensitive bank details. More than half of India's crimes are committed by fraudsters posing as bank managers and extracting money (phishing) .

Hacking "attacks that take advantage of vulnerabilities in software and services, weaknesses in protection mechanisms, and other shortcomings of targeted systems that do not involve social engineering or malware." Examples include server-based attacks or the manipulation of block chain-based services. One-fifth of the cybercrimes involved hacking. To prevent Hacking use only trusted services. Be aware of cybersquatting sites which looks similar to popular site like amzon.com instead of amazon.com. Make sure all software is up to date. Perform security audits regularly. Encrypt all the data. Enable two level authentication that is not only password and OTP to registered mobile or email. Avoid login to the new site through existing social media accounts Facebook, google account.

Web attacks : Web servers are easy to configure and manage. The software underlying webserver is complex and may hide potential security flaws[11]. Web attacks exploit vulnerabilities in websites to access the data of other users of the sites. Most of these attacks are against businesses. For example, hackers might inject malicious code into an e-commerce website that allows them to steal customers' confidential information. These attacks can be prevented using security protocol, IPSec, SSL, TLS working with trusted web developers and using trusted third party(kerberors).

Credential compromise: hacker uses your login information to gain unauthorized access to your accounts. An attacker can learn your credentials in a number of ways: phishing, social engineering, malware (such as keyloggers), or hacking (gaining access to a database of credentials and cracking the passwords). Users are suggested to choose strong, unique passwords and/or passphrases and always use services that offer two-factor authentication.

Crypto jacking[4] is unauthorized access to victim's computer to mine for crypto currency. This is achieved by sending phishing mails or making victim to click on malicious link and then by loading crypto mining

code to victims' system. It is most dangerous ransomware. Cryptomining scripts detects whether the system is already infected by any other cryptomining scripts then disables earlier one. Cryptomining scripts have kill prevention mechanism. Crypto jacking is prevented by installing ad blocking and anti-crypto mining extensions on the web browser. Use anti-virus software capable of detecting crypto-miners and keep web filtering tools update.

DDoS attack

DDoS attack (2%), these can be extremely costly and disruptive. DDoS attacks flood a network with traffic, overwhelming it and preventing legitimate users or employees from accessing the service. Once the network is effectively shut down, the hackers typically demand a ransom to restore service. Most DDoS attacks require the use of specialized services that use software to identify and divert malicious traffic.

In[8] listed leading cyber threats targeting organization on 1 to 5 scale is as given below

Cyber threat	Targeting organization on 1 to 5 scale
malware	3.74
Phishing	3.71
ransomware	3.68
Credentials abuse	3.68
DDOS	3.63
Web attacks	3.62

IV. IOT AND CYBER CRIME

The Internet of Things (IoT)[5] is networking paradigm, which allows communication among all types of physical objects (or "things") over the Internet. The development of the IoT has lead to a variety of ethical problems and discussions in society. Many of these, such as the loss of confidence, privacy violations, misuse of data, the digital divide, identity theft, access to information and control problems, freedom of speech and freedom of expression, have already arisen in connection with the use of the Internet and ICT in general.

Security issues in IOT is to protect equipment, services and information.

IOT nodes are made by different manufacturers some of them may be not reliable. Some of the attacks may occur by getting credential of the device provided for communication like device identity and keys provided at the time of installation. some the attacks are operational attacks. Cybercrime can occur at the level of end node like mobile devices, consoles, smart devices through spread of malware . Un authorized access to network and cloud leads to data theft. Type of attacks in IOT devices is UDP flood it leads to denial-of-service attack .

V.ROLE OF DIGITAL FORENSICS

In response to the cybercrime certain procedures followed are investigate or resolve it and recover quickly. Recovering the data is to minimize harm. Investigation of cybercrime focus on digital forensics. Digital forensics[6] practice identifying, collecting, analyzing and reporting on information found on computers, mobile devices and networks such that the evidence is admissible in legal context. Evidence collected in digital forensics help in incident response and remediation activities.

Various branches of digital forensics are Disk forensics, Printer Forensics, Network Forensics, Mobile Device Forensics, Database Forensics, Digital Music Forensics, Scanner Forensics, PDA Forensics and Multimedia Forensics. Disk forensics deals with extracting forensic information from storage media like hard disk,

Printer forensics deals with identification unique feature printer to identify origin of printed document . Electro -Static Detection Apparatus (ESDA), Video Spectral Comparator (VSC)are used to identify the features of document. So many image processing sophisticated tools are implemented to identify the source of document.

Network forensics deals with tracking and monitoring network traffic to make sure how the attack happens.

Mobile forensics is recovering the evidence from mobile phone using advanced methods. It is different from classical computer forensics.

Database forensics dealt with auditing of time stamps to verify the actions of database user or to identify the transactions within database. Some third-party software can be used to analyze data.

Scanner forensic is dealt with identifying model of the scanner captured scanned images. Statistical features of the scanning noise and wavelet analysis will help in scanner characterization. The same methodology can be used in digital cameras.

PDA Forensics is most challenging task compared to computer forensics. Modern Personal digital

assistance are hybrid devices integrating all wireless, mobile phone, bluetooth. Evolution of Artificial Intelligence and IOT posing more challenges in identify the evidence.

VI. CONCLUSION

Cyber security has become challenging task with evolution of Artificial Intelligence and IOT. Attackers are keep trying to exploit vulnerabilities in software and hardware. Awareness should be created among user regarding cyber threats and initiating practice of strict ethical policies while using internet or any other third-party software. Frequent backup of confidential data and change of password and use of strong fire wall will protect user from unknown cyber-attacks.

REFERENCE

[1] M. Uma and G. Padmavathi, "A Survey on Various Cyber Attacks and Their Classification," International Journal of Network Security, vol. 15, no. 1, pp. 390–396, 2013.

[2] Dr. Mike MCGuire and Samantha Dowling, Cyber Crime : A review of the evidence, research report, INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

[3] Digital evidence and computer crime: Forensic science, computer and the Internet E casey-books.google.com.

[4] https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html

[5] Dr. Algimantas Venčkauskas*, Dr. Robertas Damaševičius, Dr. Vacius Jusas, Dr. Jevgenijus Toldinas, MSc Darius Rudzika, MSc Giedrė Drėgvaitė ,A REVIEW OF CYBER-CRIME IN INTERNET OF THINGS: TECHNOLOGIES, INVESTIGATION METHODS AND DIGITAL FORENSICS, International Journal of Engineering Science and Research Technology, pg 460-477 , October 2015

[6] David Mugisha, Role and Impact of Digital Forensics in Cyber Crime investigation, Gujarat Forensic Science University, Article in International Journal of Cyber Criminology, March 2019.

[7] https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html

[8] https://financesonline.com/cybercrime-trends/

[9] G.Nikhitha Reddy and G.J. Ugander reddy , A Study of Cyber Security Challenges and Its Emerging Trends on Latest Technologies

[10] Dr.Prof. Rajasekharaiah K.M , Chhaya S Dule and Sudarshan E , Cyber Security Challenges and its Emerging Trends on Latest Technologies, IOP Conf. Series: Materials Science and Engineering, IOP Publishing, December 2020

[11] William Stalling, Cryptography and Network Security Principles and Practices, Fourth Edition, Prentice Hall