International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 08 | Aug 2022 www.irjet.net p-ISSN: 2395-0072

A Review Paper on Cyber-Security

Aishwarya Pradeep Zope[1], Rashmi Rajendra Chaudhari[2]

[1] Passed Out Student, Dept. of Computer Engineering, Government College of Engineering, Jalgaon
[2] Visiting Faculty, Dept. of Computer Engineering, Government College of Engineering, Jalgaon

---

Abstract: *Internet, the worldwide connection of loosely held networks, has made the flow of data and information between different networks easier. With data and information being transferred between networks at distant locations, security issues have become a major concern from the past few years. The internet has also been used by few people for criminal activities like unauthorized access to others networks, scams, etc. These criminal activities related to the internet are termed as Cyber Crimes. With the increasing popularity of online activities like online banking, online shopping, etc., it is a term that we often hear in the news now-a-days. Therefore, in order to stop and punish the cyber criminals, "Cyber Law" was introduced. Cyber Law can be defined as law of the web, i.e., it is a part of the legal systems that deals with the Internet, Cyberspace and with other legal issues like online security or online privacy.*

Therefore, keeping the objectives in mind, this chapter is divided into different sections in order to provide a brief overview of what is cybercrime, the perpetrators of cybercrime-hackers and crackers, different types of cybercrimes and the evolution of cyber laws in India. The chapter further throws light on how these laws work and the various preventive measures which can be used to combat this "hi-tech" crime in India.

Keywords:- Cybercrime, Cyber-Security,Hacking, Trojans, Worms, Botnets, Phishing, Keylogger attacks, Brute-force attacks.

1.INTRODUCTION

Cyber-attacks are taking place all the time; even as we speak security of some organizations big or small is being compromised. For example, if you visit the site 'threat cloud' we can view all the cyber-attacks that are happening right now. It gives us the scale of actual cyber-attacks happening all the time in the world.Nowadays we use the internet for many day-to-day activities. However, we need to stay alert to the notifications we receive and about the system. With the advancement in Information Technology, the way cybercriminals commit the crime is also changing day by day.

2.DEFINITION

Cyber Crime:-Cybercrime or computer crime is a criminal activity that involves unlawful access to computer systems. It is an illegal activity committed over the internet.

Definition:-

The word "cyber" is slang fr anything relating to computers, Information Technology, and virtual reality. Therefore, is stans to reason that "cybercrime" are offences relating to computers, Information Technology, the internet, and virtual reality.

Crime committed using a computer and the internet to steal data and information is a cybercrime.

3.EXAMPLEs:-

1). Stealing credit card information.

2). Breaking into the government website

3). Email and Internet fraud.

4). Identity fraud.

5). Theft and sale of corporate data.

6). Ransomeware attacks.

7). Cyberextortion(demanding money to prevent a threatened attack).

8). Cyber Spying (where hackers access government or company data).

9). Cryptojacking(where hackers mine cryptocurrency using the resources they do not own).

4.HISTORY:-

The exact origin of cybercrime, the very first instance in which someone committed a crime across a computer network, is impossible to know.

The first case of use of computer theft was in 1973, A teller at a local New-York bank used a computer to embezzle over 2 million dollars.

The first spam email took place in the year 1978. Sending spam emails is a cybercrime. In certain countries, we can be behind bars if we send spam emails.

In 1980's MNC Database (pentagon and IDM) was hacked.

The first virus was installed on Apple computers was in the year 1982.

In 1981, Ian Murphy, known as Captain Zap was the first person convicted of cybercrime. He hacked into the AT&T network and changed the internal clock to charge off-hours rates at peak times. He received 1,000 hours of community service and 2.5 years of probation.

In 1990's National crackdown on criminals and Microsoft's NT operating system pierced. This is where hacking started to become main stream. Before this, hacking was very much limited to organisation.

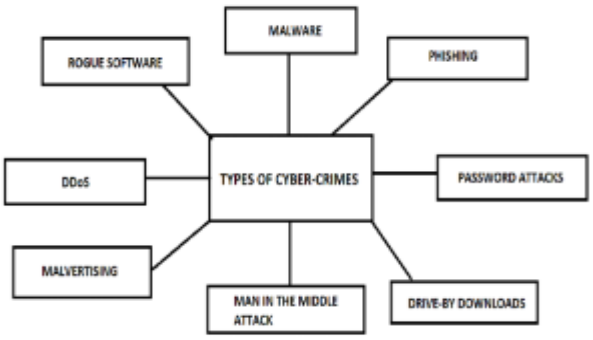
In 2001, Cybercriminals launched attacks against eBay, Yahoo, CNN.com, amazon and others.

In 2007, Bank hit by biggest ever hack. Swedish bank, Nordea recorded nearly $1 Million has been stolen in three months from 250 accounts.

In 2013, Adobe had 2.9million accounts compromised and their usernames and passwords were released on the open internet.

In 2016, Kaspersky: one of the leading antivirus providers to the world reported around 758 million malicious attacks that occurred .

5.TYPES OF CYBERCRIME:-



5.1 MALWARE ATTACKS:-

It is an attack where a computer system or network is infected with a computer virus or other type of malware. It is an all-encompassing term for a variety of cyberattacks including trojan viruses. It is defined as code with malicious intent that typically steals data or destroys something on the computer.

A famous example of a malware attack is the WannaCry ransomware attack, a global cybercrime committed in May 2017.

When the WannaCry ransomware attack hit, 230,000 computers were affected across 150 countries. Users were locked out of their files and sent a message demanding that they pay a BitCoin ransom to regain access.

Many cyber criminals use computer viruses to gain unauthorized access to systems and steal data. A computer virus is a malware(malicious software program) loaded into a computer without the knowledge of the user.

5.1.1 Viruses:-

Like its biological name says viruses attach themselves to clean files and infect other clean files and they can spread uncontrollably damaging a system's core functionality and deleting or corrupting files. They usually appear as an executable file that you might have downloaded from the internet.

5.1.2 Trojans:-

This kind of malware disguises itself as legitimate software or is included in legitimate software that can be tampered with. It tends to act discretely and creates backdoors in our security to let other malware enter our system.

5.1.3 Worms:-

Worms infect entire networks of devices either local or across the internet by using the network interfaces. It uses each consecutive infected machine to infect more.

5.1.4 Botnets:-

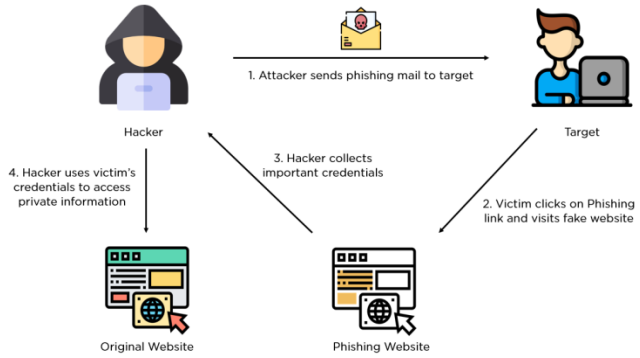
Botnets are networks of infected computers that are made to work together under the controller of an attacker.

We can encounter malware if we have os vulnerabilities or if we download some l legitimate software from somewhere or we have some email attachments that were compromised with.

5.2 PHISHING:-

It is a cybercrime where people are contacted through phone calls, email, or a message by cybercriminals posing as a person from a legitimate institution. A phishing campaign is when spam emails, or other forms of communication, are sent emails, to trick recipients into doing something that undermines the security or security of the organization they work for. These cybercriminals collect personal information like bank account details and passwords and then steal money. Messages sent by phishing look authentic and attempt to get victims to reveal their information.

Phishing working:-



The attacker must decide which business to target and determine how to get the email address of the customers of that business. Then they go through a setup phase; once they know which business to spoof and who their victims are attackers create methods for delivering the messages and collecting the information; then they execute the attack. After that attacker records the information the victims enter into the webpage or pop-up windows and in the last step which is identity theft and fraud the attacker uses the information they have gathered to make illegal purchases or commit fraud.

5.3 PASSWORD ATTACK:-

It is an attempt to obtain or decrypt a user's password for illegal use. Hackers can use cracking programs, dictionary attacks, and password sniffers in password attacks. Defence against password attacks is rather limited but usually consists of a password policy including a minimum length, unrecognizable words, and frequent changes.

This attack can be done for several reasons but the most malicious reason is to gain unauthorized access to a computer without the computer's owner's awareness not being in place; so this results in cybercrime such as stealing passwords to access bank information. There are three common methods used to break into a password-protected system.

1). Brute-force attack: In this, a hacker uses a computer program or script to try to log in with possible password combinations usually starting with the easiest to guess password.

2). Dictionary attacks:- In this, a hacker uses a program or script and tries to log in by cycling through the combinations of common words. This attack tries only those possibilities which are most likely to succeed; typically derived from a list of words; for example dictionary.

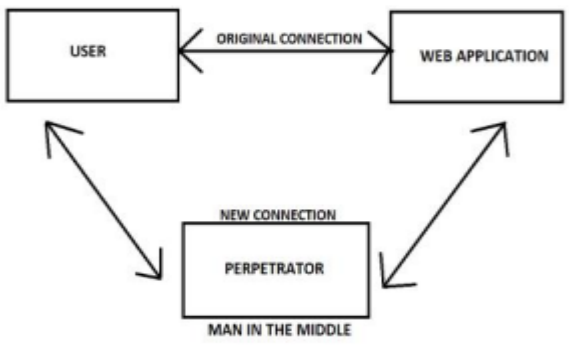
These attacks are more successful because people tend to choose easy passwords like their names, birthdates, etc.

3). Keylogger attacks:- In this, the hacker uses a program to track all of the user's keystrokes; so at the end of the day, everything the user has typed including the login IDs and passwords has been recorded.

5.4 DISTRIBUTED DoS ATTACK

Distributed DDoS attacks are a type of cybercrime attack that cybercriminals use to bring down a system or network. Sometimes connected IoT devices are used to launch DDoS attacks. In this attacker sends a high volume of data of traffic through the network until the network becomes overloaded and can no longer function

5.5 MAN IN THE MIDDLE ATTACK:-



This attack can obtain information from the end-user and the entity he or she is communicating with.

For example, if you are banking online the man in the middle would communicate with you by impersonating your bank and communicate with your bank by impersonating you. The man in the middle would receive all of the information transferred between both parties which could include sensitive data such as bank accounts and personal information.

5.5.1 PREVENTION OF MITM

1). Use encrypted WAP(Wireless Access Point)

2). Always check the security of your connection. (HTTPS or HSTS)

3). Invest in VPN.

DRIVE-by Download:-This attack occurs when vulnerable computers get infected by just visiting a website.

Findings from the latest Microsoft Security Intelligence Report reveal that this attack has become the top web security threat to worry about.

5.6 ROGUE SOFTWARE:-

This is also called rogue security. It is designed specifically to damage or disrupt a computer system. In this case, not only is the software going to disrupt your system, it's going to try and trick you into making a purchase using your credit card.

Other ways to fool the people are as follows:-

1). Hacking:- This is one form of cybercrime in which you get into somebody's system and then try to use information, disrupt the working, disrupt the network, etc.

2). Credit card fraud:- The most common fraud performed under cybercrime is credit card fraud which happens over the internet, through the call centers, and lot many ways.

3). Virus disssemination:-Installing, sending viruses via the network, vis emails, via messages, etc is one of the more common types of cybercrime.

4).computer vandalism:- is getting a lot of people involved nowadays.

5). Software piracy:-The unauthorized copying, distribution, or use of the software is called software piracy. Cybercriminals distribute pirated software which causes loss to the software company. Southeast Asia is considered one of the bigger markets of software piracy.

6). Identity theft:- It is a cybercrime where cybercriminals steal personal data like passwords or bank account details.

7). Cyber bullying:- It is a form of online harassment of a person using smartphones or computers. It is also known as cyber harassment or online bullying. Cyberbullying generally occurs on platforms like social media and gaming platforms. It involves posting hate comments and sharing negative information about a person.

6. CYBERCRIME AND INFORMATION SECURITY

Information security is a potential activity by which information and other communication systems are protected from and/or defended against unauthorized use or modification or exploitation or even theft.

6.1 Some steps that we can use to avoid being a victim of cybercrimes are:-

1). Keep Software and operating systems updated:-

Keeping your software and operating systems up to date ensures that you benefit from the latest security patches to protect your computer.

2). Manage your social media settings:-

Keep your personal and private information locked down. Social Engineering cybercriminals can often get your personal information with just a few data points. For instance, if you post your pet's name, you might expose the answers to common security questions.

3). Use Anti-Virus software and keep it updated

This is the smart way to protect your system from attacks.

4). Use strong passwords:-

Be sure to use strong passwords that people will not guess and do not record them anywhere. Or use a reputable password manager to generate strong passwords randomly to make this easier.

5). Do not click on links in spam emails or untrusted websites:-

Another way people become victims of cybercrime is by clicking on links in spam emails or other messages, or unfamiliar websites.

6). Be mindful of which website URLs you visit.

Keep an eye on the URLs you are clicking on. Avoid clicking on links with unfamiliar or spammy-looking URLs.

1). Avoid the use of public wi-fi networks.

2). Avoid using public computers while doing financial transactions.

3). Never share your passwords with anyone.

4). Avoid downloading unknown applications on your system.

7. SOME KEY POINTS OF THE INFORMATION TECHNOLOGY (IT) ACT, 2000 ARE AS FOLLOWS:

E-mail is now considered a valid and legal form of communication.

Digital signatures are given legal validity within the Act.

The Act has given birth to new business companies to issue digital certificates by becoming the Certifying Authorities.

This Act allows the government to issue notices on the internet through e-governance.

Communication between the companies or between the company and the government can now be through the internet also.

Addressing the issue of security is the most important feature of this Act. It introduced the concept of digital signatures that verifies the identity of an individual on the internet.

In case of any loss or harm done to the company by criminals, the Act provides a remedy in the form of money to the company.

Apart from the above-mentioned Sections under the IPC and ITAA, 2008, the Government of India has taken the following steps for the prevention of Cybercrimes:

Cybercrime cells have been set up in states and U.T's for reporting and investigation of Cybercrime cases.

The Government under the IT Act, of 2000 has also set up *Cyber forensics and Training Labs* in the states of Kerala, Assam, Mumbai, Mizoram, Manipur, Nagaland, Arunachal Pradesh, etc., for awareness creation and training against Cybercrimes.

In collaboration with the Data Security Council of India (DSCI), NASSCOM, *and Cyber Forensic Labs* have been set up in Mumbai, Bengaluru, Pune, and Kolkata for awareness creation and training.

8. CYBERSECURITY

It is the technology and process that is designed to protect networks and devices from attack, damage, or unauthorized access.

ADVANTAGES:

1).Protection of our business.

2).Increased productivity

3).Inspires customer confidence.

4).Stops your website from crashing.

5).Protection for your customers or clients.

9. WHY DO WE NEED CYBERSECURITY?

Three main pillars of cyber security are:-

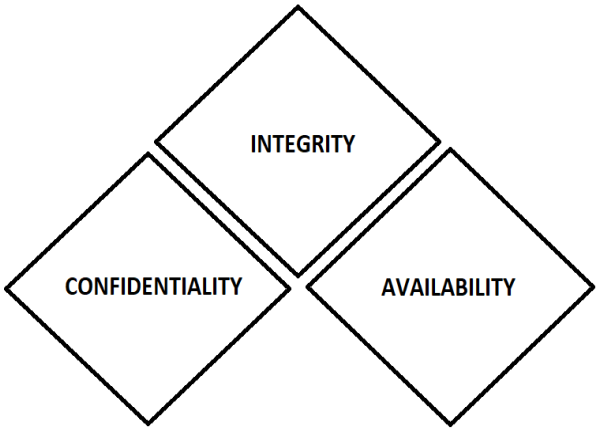


Fig:- 3 main pillars of cyber security

1).Confidentiality:- (Data should be confidential) the principal of confidentiality asserts that the information and functions can be accessed only by authorized party.

2).Integrity:- (Data Integrity should ne intact) the principles of integrity assert that information and functions can be added, altered, or removed only by authorized people and means.

3).Availability:- (Data should be available) the principles of availability assert that systems, functions, and data must be available on demand according to agreed-upon parameters based on levels of service.

10. MOTIVES BEHIND CYBERCRIME:-

1). Disrupting business continuity.

2). Information theft and manipulating data.

3).Creating fear and chaos by disrupting critical infrastructure.

4). Financial loss to the target.