ASANSOL ENGINEERING COLLEGE

Various Kinds of Cyber Threats & Attacks

Presented by
AISHWARYA GHOSH
ROLL NO.- 10800219074
REG NO.- 036064 OF 2019-20
YEAR- 4TH (8TH SEM)

SUB- CRYPTOGRAPHY AND NETWORK SECURITY
SUB CODE- PEC – IT801B

YEAR 2023

DEPARTMENT OF INFORMATION TECHNOLOGY

OVERVIEW

Threat is a possible security violation that might exploit the vulnerability of a system or asset. The origin of the threat may be accidental, environmental (natural disaster), human negligence, or human failure. Attack is a deliberate unauthorized action on a system or asset. Attacks can be classified as active and passive attacks. Threat and attacks are two important events from a security perspective.

CYBER THREATS AND ATTACKS

- **CYBER THREATS**:-

A cyber security threat refers to any possible malicious attack that seeks to unlawfully access data, disrupt digital operations or damage information. A cyber attack is an intentional and malicious effort by an organization or an individual to breach the systems of another organization or individual.

- **CYBER ATTACKS**:-

A cyber attack is a set of actions performed by threat actors, who try to gain unauthorized access, steal data or cause damage to computers, computer networks, or other computing systems. The individuals who launch cyber attacks are usually referred to as cybercriminals, threat actors, bad actors, or hackers.

EXAMPLE

1. Malware:-

Malware is malicious software such as spyware, ransomware, viruses and worms. Malware is activated when a user clicks on a malicious link or attachment, which leads to installing dangerous software. Cisco reports that malware, once activated, can:

- Block access to key network components (ransomware)
- Install additional harmful software
- Covertly obtain information by transmitting data from the hard drive (spyware)
- Disrupt individual parts, making the system inoperable

The malware landscape evolves very quickly, but the most prevalent forms of malware are:

1. Botnet Malware - adds infected systems to a botnet, allowing attackers to use them for criminal activity.

2. Cryptominers - mines cryptocurrency using the target’s computer.

3. Infostealers - collects sensitive information on the target’s computer.

4. Banking trojans - steals financial and credential information for banking websites.

5. Mobile Malware - targets devices via apps or SMS.

6. Rootkits - gives the attacker complete control over a device’s operating system.

2. Emotet:-

The Cybersecurity and Infrastructure Security Agency (CISA) describes Emotet as “an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans. Emotet continues to be among the most costly and destructive malware.”

3. Denial of Service:-

A denial of service (DoS) is a type of cyber attack that floods a computer or network so it can’t respond to requests. A distributed DoS (DDoS) does the same thing, but the attack originates from a computer network. Several other techniques may be used, and some cyber attackers use the time that a network is disabled to launch other attacks. A botnet is a type of DDoS in which millions of systems can be infected with malware and controlled by a hacker. Botnets sometimes called zombie systems, target and overwhelm a target’s processing capabilities.

4. Man in the Middle:-

A man-in-the-middle (MITM) attack occurs when hackers insert themselves into a two-party transaction. After interrupting the traffic, they can filter and steal data, according to Cisco. MITM attacks often occur when a visitor uses an unsecured public Wi-Fi network. Attackers insert themselves between the visitor and the network, and then use malware to install software and use data maliciously.

5. Phishing:-

Phishing attacks use fake communication, such as an email, to trick the receiver into opening it and carrying out the instructions inside, such as providing a credit card number. “The goal is to steal sensitive data like credit card and login information or to install malware on the victim’s machine,” Cisco reports.

6. SQL Injection:-

A Structured Query Language (SQL) injection is a type of cyber attack that results from inserting malicious code into a server that uses SQL. When infected, the server releases information. Submitting the malicious code can be as simple as entering it into a vulnerable website search box.

7. Password Attacks:-

With the right password, a cyber attacker has access to a wealth of information. Social engineering is a type of password attack that Data Insider defines as “a strategy cyber attackers use that relies heavily on human interaction and often involves tricking people into breaking standard security practices.” Other types of password attacks include accessing a password database or outright guessing.

DIFFERENCE BETWEEN THREAT AND ATTACK

THREAT	ATTACK
Circumstance that has the ability to cause damage.	Objective is to cause damage
Information may or may not be altered or damaged.	Chance for information alteration and damage is very high.
It can be intentional or unintentional.	It is intentional.
It may or may not be malicious.	It is malicious.
It can be classified into Physical threat, internal threat, external threat, human threat, and non-physical threat.	It can be classified into Virus, Spyware, Phishing, Worms, Spam, Botnets, DoS attacks, Ransom ware, Breaches.

CYBER ATTACK PREVENTION

1. **Web Application Firewall (WAF)** can block malicious traffic before it reaches a web application, and can prevent attackers from exploiting many common vulnerabilities.

2. **DDoS Protection** system or service monitors traffic to detect a DDoS attack pattern, and distinguish legitimate from malicious traffic.

3. **Bot Protection** system detects and blocks bad bots, while allowing legitimate bots to perform activities like search indexing, testing and performance monitoring.

4. **Cloud Security** providers take responsibility for securing their infrastructure, and offer built-in security tools that can help cloud users secure their data and workloads.

5. Database Security solutions can help ensure a consistent level of security for databases across the organization.

6. API Security automated API protection ensures your API endpoints are protected as they are published, shielding your applications from exploitation.

7. **Threat intelligence** databases contain structured information, gathered from a variety of sources, about threat actors, attack tactics, techniques, and procedures, and known vulnerabilities in computing systems.

THANK YOU