

Types of Cyber Threats

Agenda

- What are **Cyber Threats**?
- Types of **Cyber Threats**
 - i. Phishing attack
 - ii. SQL injection threat
 - iii. Man-in-the-middle attack
 - iv. Malware
 - v. Zero-day attack
 - vi. Cross-site-scripting
 - vii. Advanced persistent threats
 - viii. Password attack
 - ix. Drive by attack
 - x. Denial of service attack
 - xi. Distributed denial of service attack
 - xii. Eavesdropping attack
 - xiii. AI-powered attack
- Cyber threat intelligence



What are Cyber Threats?

What are Cyber Threats?

Cyber Threats are malicious attacks that damage and steal data which in turn affects the digital life.

Sources of Cyber Threats

- State-sponsored
- Terrorists
- Industrial spies
- Organized crime groups
- Hackers
- Hacktivists
- Cyber espionage



Types of Cyber Threats

Types of Cyber Threats

- **Phishing** attack
- **SQL Injection** threat
- **Man-in-the-middle** attack
- **Malware**
- **Zero-day** attack
- **Cross-site-scripting**
- **Advanced persistent threats**
- **Password** attack
- **Drive by** attack
- **Denial of service** attack



Phishing attack

Phishing is the technique to steal a user's data from the internet or computer-connected device.

Types of Phishing attacks

- Phishing email
- Domain spoofing
- Voice phishing
- SMS phishing
- Clone phishing
- Typosquatting
- Evil twin
- Whale phishing

Phishing attack

Ways to prevent Phishing attack

- Know what a phishing scam looks like
- Don't click on a random link
- Get free anti-phishing add-ons
- Don't give your information to an unsecured site
- Change passwords regularly
- Install firewalls



SQL injection threat

In the SQL injection threat, the attacker sends a malicious query to the device or a server. The server is then forced to expose sensitive information.

Ways to prevent SQL injection threat

- Validate user inputs
- Sanitize data by limiting special characters
- Use stored procedures in the database
- Establish appropriate privileges and strict



Man-in-the-middle attack

The man-in-the-middle attack is a security breach where cybercriminals place themselves between the communication system of a client and the server.

Types of Man-in-the-middle attack

- Session hijacking
- IP spoofing
- Replay

Ways to prevent Man-in-the-middle attack

- Strong router login credentials
- Virtual private network

Malware

Malware is a malicious software which gets installed into the system when the user clicks on a dangerous link or an email.

Types of Malware

- Viruses
- Trojans
- Worms
- Ransomware



Ways to prevent Malware

- Regularly update your computer and software

- Be careful while opening unknown email attachments or images

Zero-day attack

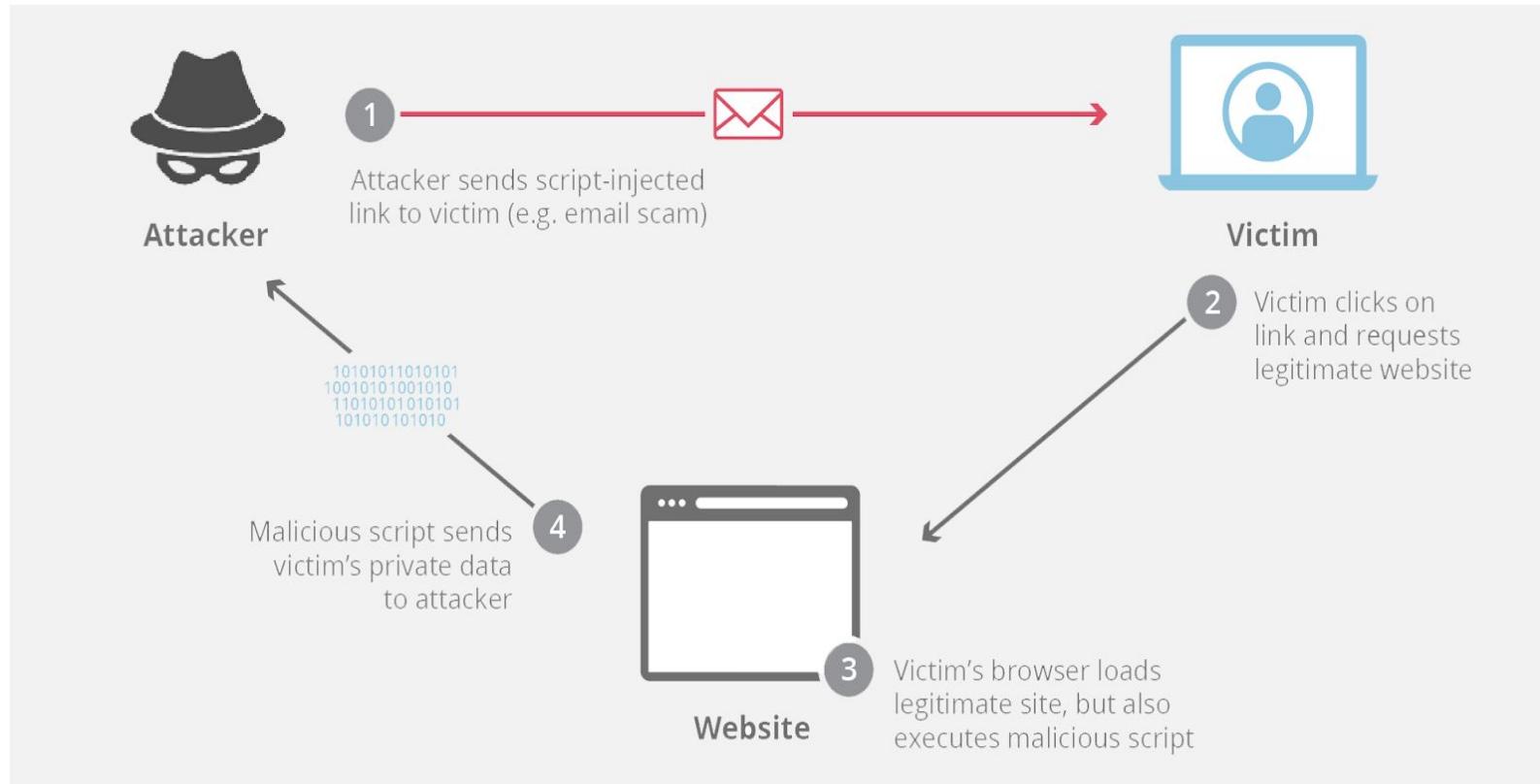
A zero-day attack is an attack done by hackers when the network, hardware or software vulnerability is announced publicly.

Ways to prevent Zero-day Attack

- Use an advanced, proactive email security solution
- Educate users
- Deploy a web application firewall
- Implement network access control

Cross-site-scripting

Cross-site scripting is a cyber-attack where an attacker sends malicious code to a reputable website.



Cross-site-scripting

Ways to prevent Cross-site-scripting

- Filter input on arrival.
- Encode data on output.
- Use appropriate response headers.
- Content security policy.



Advanced persistent threats

An advanced persistent threat occurs when an attacker gains unauthorized access to a system or network and remains undetected for a long duration.

Ways to prevent Advanced persistent threats

- Install a firewall
- Enable a web application firewall
- Install an antivirus
- Implement intrusion prevention systems
- Create a sandboxing environment
- Install a VPN



Password attack

Password attack is an attempt to steal passwords from a user.

Two common techniques used to get user's password

- Brute-force guessing
- Dictionary attack



Ways to prevent Password attack

- Use strong password
- Multi-factor authentication

Few other types of Cyber Threats

- Drive by attack
- Denial of service
- Distributed denial of service
- Eavesdropping attack
- AI-powered attack



Cyber threat intelligence

Cyber threat intelligence is the amount of data that becomes cyber threat information that is collected, evaluated in the context of its source, and analyzed through rigorous and firm tradecraft techniques by the industry experts.



Summary

Thank You