Cyber Attacks

In this article, we'll review common and dangerous cyber attacks.

What We'll Be Learning

Imagine we are in an interview for our first Cybersecurity job. During the interview, the interviewer asks, "You must have done research about our company, what we do, what we produce, and what kind of threats we face every day. Based on your research, can you tell the most dangerous attacks our company could face?"

To answer a question like this, it's helpful to know what common attacks are.

Before we review the most dangerous attacks, we will review some of the most common cyber attacks:

- Application Attacks
- Network Attacks
- Malware Attacks
- Overflow Attacks
- Password Attacks
- Social Engineering Attacks

Next, we will discuss the most dangerous cyber attacks. These cyber attacks include:

- Improper session handling
- Ransomware exfiltration and extortion
- Supply chain attacks
- Adversarial machine learning attacks

Most common cyber attacks

First, we must answer the question: what are cyber attacks?

Cyber attacks can be defined as when threat actors use special techniques to exploit vulnerabilities in applications, processes, or procedures.

Web Application Attacks

In Web Application Attacks, the adversaries exploit vulnerabilities of the services running on the web server infrastructure. The infrastructure could include web apps, database servers, etc. These elements could be both on the internet or inside the company's networks (intranet).

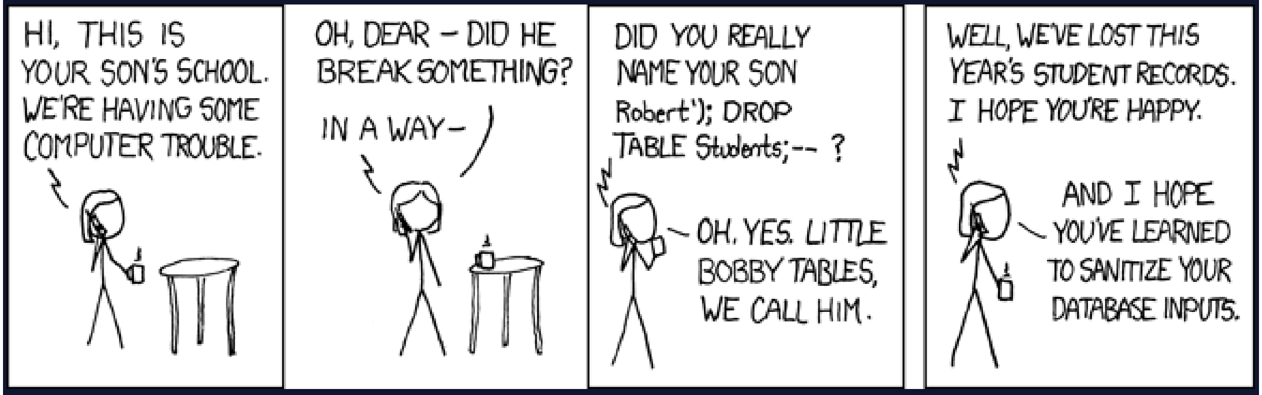
The attackers can use the following techniques to exploit web services:

Cross-Site Scripting

Cross-Site Scripting (XSS) is an attack where an attacker injects malicious code on a website that delivers the script to the victim's browser.

Injection Attacks

In a SQL Injection Attack, the attackers input SQL commands into a webpage to retrieve sensitive data from the database. If user input is properly validated and sanitized, SQL injection attacks shouldn't work.


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

xkcd comic "Exploits of a Mom"

In an XML Injection attack, the attackers manipulate a NoSQL database using XML instead of SQL commands.

Network Attacks

In Network Attacks, the adversaries exploit vulnerabilities of applications or devices (firewalls, routers, and switches) in the intranet to ultimately gain access to internal systems.

Some examples of network attack techniques are:

- **Man-in-the-Middle (MitM)/on-path/eavesdropping attacks**: the attackers intercept communication between the client and server applications and impersonate one of them to read or tamper with the information.
- **DNS Attacks**: as DNS traffic is rarely blocked, the attackers utilize the DNS protocol to exfiltrate data from an internal system.
- **DoS Attacks**: the attacker floods networks or systems with traffic to exhaust all its resources or bandwidth, resulting in the devices' inability to process legitimate requests.

Malware Attacks

Malware is malicious software designed for compromising systems or devices in the network.

There are many types of Malware, and some particularly dangerous types are:

- **Ransomware** denies access to business data by encrypting them. We will discuss more ransomware attacks later in this article.
- **Backdoor**s establish persistence so the attackers can covertly maneuver between systems.
- **Spyware** covertly collects information and transmits the data to remote locations of choice by the attacker.
- A **logic bomb**, as the name suggests, waits for a specific logical event to happen before executing its intended purpose.
- A **rootkit** operates in the lower level of the operating systems to evade antivirus.

Password Attacks

In Password Attacks, the attackers often attempt to access systems with compromised passwords.

Password Attacks could be:

- In password **brute-forcing attacks**, the attackers use **password spraying** techniques to use one password against many usernames. This technique favors the attacker by avoiding account lockouts.

- In **credential harvesting**, the attackers use a collection of stolen usernames and passwords to access the target systems.

Buffer Overflow Attacks

In Buffer Overflow Attacks, an attacker feeds well-crafted input into a program’s fixed-length storage buffer causing malicious code, including the intended “return address,” to be written and executed from the adjacent memory locations.

Buffer overflows could be overflowing the stack (stores local variables) or heap (handles dynamic allocation of memory) area of the memory.

Social Engineering Attacks

An attacker uses social skills to compromise information about the organization or its assets in social engineering attacks.

Types of social engineering attacks could include:

- **Phishing** attack, where the attackers send an email that appears to be from a reputable source, often soliciting personal information
- In a **vishing** attack, the attackers use voice communication, most often spoofing the caller identity of the Voice over Internet Protocol (VoIP) phone services.
- A **smishing** attack uses SMS or text messages to send malicious links to the victims.

Most dangerous new attacks

Session hijacking/Improper handling

Session hijacking or improper handling occurs when the session token used to facilitate a stateful transaction is unintentionally shared with the attackers. The attackers with access to the session tokens from a privileged user can issue administrative actions that could be very dangerous. The scope of cyberspace has increased significantly due to the range of applications in use to support remote work. As these applications are not originally designed to be used in remote environments, the adversaries can easily grab tokens from unclosed sessions in the remote worker’s environment and impersonate them to conduct fraud or information theft.

Double extortion ransomware attacks

Traditionally, a ransomware attack is a denial-of-service attack where the attackers encrypt critical data and demand a ransom to end the attack. But in the new ransomware attacks, the adversary first exfiltrates the important data and then threatens to leak the sensitive data publicly if the victim denies paying the ransom. This type of ransomware attack is called double extortion ransomware attack. The cyber attack on Colonial Pipeline ransomware attack is an example of this kind of attack.

Adversarial machine Learning attacks

As vendors are heavily using machine learning capabilities to detect and classify good vs. bad data, the attackers are using Adversarial Machine Learning (AML) attacks to evade these capabilities. Researchers train the ML models with malware samples that possibly come from adversaries. The attackers can easily poison these training datasets so the malicious programs can evade detection. Additionally, the adversary can reverse engineer the ML capability by sending malware to analyze how the model classifies this malware. Then the attacker can craft malicious instances that the ML product can not recognize and classify as safe to pass through. More about AML attacks can be found in Machine Learning Security: Threats, Countermeasures, and Evaluations.

Software supply chain attacks

In software supply chain attacks, adversaries seek to compromise a vendor’s network and inject malicious code into the software. The customer also gets compromised when they download the software with malicious code. SolarWinds is an attack that compromised hundreds of companies and government agencies.

IoT devices in cyber attacks

Due to various resource constraints, traditional security measures can not be implemented in IoT devices. As a result, IoT devices are often the prime target to be used in cyber attacks. For example, in the Mirai botnet attack, they were used as bots to conduct Distributed DoS attacks.

Conclusion

In this article, we have learned about the most common and most dangerous cyber attacks.