

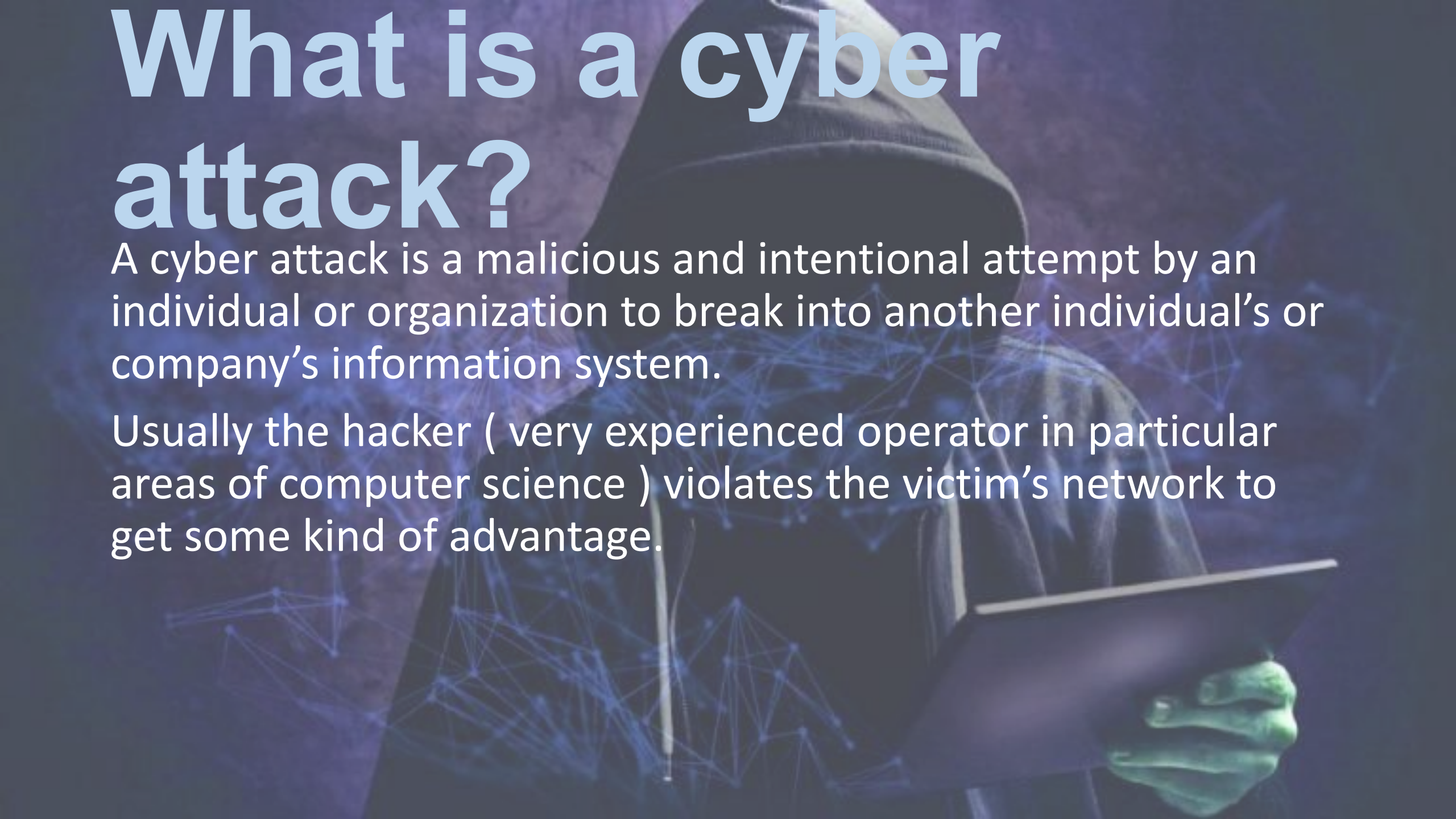


THE RISKS OF THE NETWORK

What is a cyber attack?

A cyber attack is a malicious and intentional attempt by an individual or organization to break into another individual's or company's information system.

Usually the hacker (very experienced operator in particular areas of computer science) violates the victim's network to get some kind of advantage.



A digital hand, composed of blue wireframe points and lines, hovers over a laptop keyboard. The hand is positioned as if about to type. The background is dark, and the laptop keyboard is visible in the foreground.

**Most common types of
cyber attacks**

Malware

The term malware defines «bad» software, such as spyware, ransomware, viruses and worms. Malware violates a network by exploiting a vulnerability, typically when a user selects a dangerous link or opens an email attachment that installs malicious software.

once entered the system the malware can :

- 1) Block access to the main components of the network (ransomware)
- 2) Install malware or other malicious software
- 3) Get information secretly by transmitting data from hard drive (spyware)
- 4) Interfering with certain components and making the system unusable

Phishing



Phishing consists of sending fraudulent communications that seem to come from a reliable source, usually an email. The purpose is to seize sensitive data such as credit cards and access information, or to install malware on the victim's computer. Phishing is an increasingly common cyber threat.

Attack man in the middle

Man in the middle (mitm) attacks, also known as interception attacks, occur when hackers enter a transaction between two parties. Once they have stopped traffic, criminals can filter and steal data.

There are two common entry points for mitm attacks:

1. Unsafe public Wi-Fi networks, where hackers can insert themselves between a visitor's device and the network. Without knowing it, the visitor passes all the information to the hacker.
2. Once the malware has breached a device, a hacker may install the software to process all of the victim's data.

denial-of-service attack

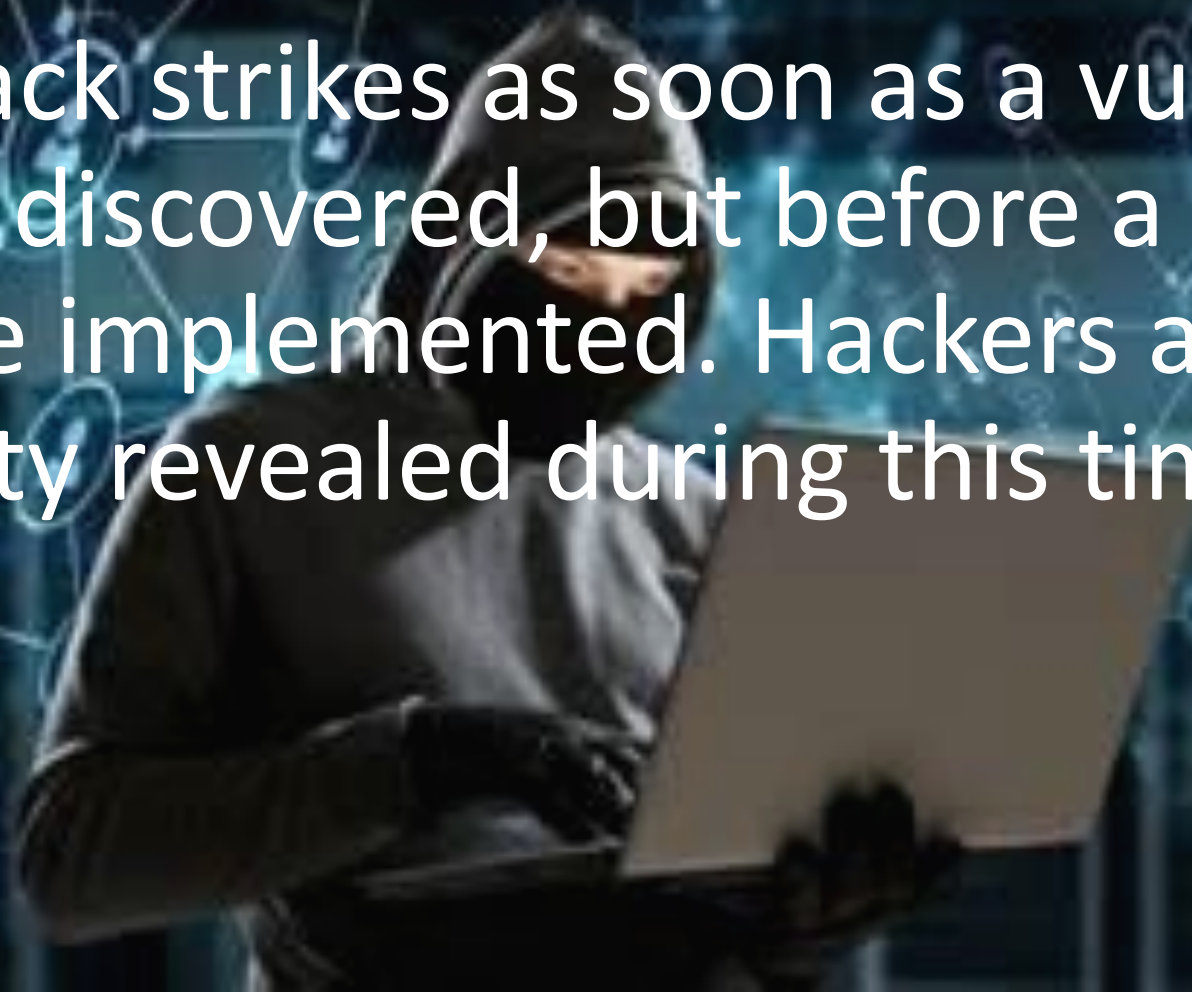
A denial-of-service attack sends massive traffic flows to systems, servers, or networks to exhaust their resources and bandwidth. As a result, the system under attack is no longer able to meet the legitimate demands. To launch such an attack, hackers can also use multiple compromised devices.

SQL injection

A Structured Query Language (SQL) injection occurs when a hacker inserts malicious code into a server that uses SQL and forces it to make public information that should normally remain confidential. To perform a SQL injection, simply add malicious code to the entry box of a vulnerable website.

zero-day attacks

A zero-day attack strikes as soon as a vulnerability in the network is discovered, but before a patch or solution can be implemented. Hackers are targeting the vulnerability revealed during this time window.



Tunneling DNS

DNS tunneling uses the DNS protocol to transmit non-dns traffic to port 53. Use DNS to send traffic with the HTTP protocol and other protocols. There are several legitimate reasons to use DNS tunneling. However, DNS tunneling services over VPNs are also used for malicious reasons. For example, they can serve to disguise outgoing traffic as DNS, hiding data that is normally shared over an Internet connection. If the use is malicious, DNS requests are manipulated to exfiltrate data from a compromised system and redirect it to the hacker's infrastructure. Tunneling can also be used for command and control callbacks from the hacker's infrastructure to a compromised system.

The background image shows a computer room with several workstations, each consisting of a monitor and a keyboard. The room is dimly lit, with a strong blue glow emanating from the background, creating a futuristic atmosphere. The floor is covered with a pattern of binary code (0s and 1s).

STEFANO TROPEA RAFFAELE VISCOMI