Cyber attacks

What’s the difference?

Cybercriminals use many different types of malicious software, or malware to carry out attacks. Malware is any code that can be used to steal data, bypass access controls or cause harm to or compromise a stystem.

Virus

Type of computer program that, **when executed, replicates and attaches itself to other files**, such as a legitimate program, by inserting its own code into it.

Some viruses are harmless yet others can be destructive.

**Most viruses requure end-user interaction to initiate activation**, and can be written to act on a specific data or time.

*Viruses can be spread through* removable media, internet downloads and email attachments.

The simple act of opening a file or executing a specific program can trigger a virus.

Once a virus is active, it will usually infect other programs on the computer or other computers on the network.

**Viruses mutate to avoid detection**.

Worms

Malicious software program that **replicates by independently exploiting vulnerabilities in networks.**

Unlike a virus, which requifres a host program to run, worms **can run by themselve**s.

Other that the initial infection of the host, they **do not require user participation** and **can spread very quickly over the network**, usually slowing it down.

Worms share similar patterns: they exploit system vulnerabilities,

They have a way to propagate themselves

They all contain malicious code to cause dmg to pc/netw

Trojan horse

Malware that **carries out malicious operations by masking its true intent**.

*It might appear legitimate but is, in fact, very dangerous*.

**It exploits the privileges of the user who runs them**.

They do not self-replicate but often bind themselves to non-executable files, such as img,… acting as a decoy to harm the systems of unsuspecting users.

Logic bomb

Is a **malicious program that waits for a trigger***, such as a specified date or database entry*, **to**  **set off the malicious code**.

**Until trigger event happens, the logic bomb will remain inactive**.

Once active, **it implements a malicious code that causes harm to a PC in various ways**, it can sabotage database records, erase files and attack operating sys. Or applications.

Cybersecurity specialists have recently discovered logic bombs that attack and destroy the hardware components in a device or server, including the cooling fans, CPU, RAM, HDD, PSU it overdrives these components until they overheat or fail.

Ransomware

**Malware** is **designed to hold a PC system or the data it contains captive until a payment is made.**

Ransomware **usually works by encrypting your data so that you cannot access it**.

*According to ransomware claims, once the ransom is paid* via an untraceable payment system, the *cybercriminal will supply a program that decrypts the files or send an unlock code* - but in reality, many victims do not gain access to their data even after they have paid.

Some versions of ransomware can take advantage of specific system vulnerabilities to lock it down.

**Ransomware is often spread through phishing emails** that encourage you to download a malicious attachment, or through a software vulnerability.

Denial of service attacks

(DoS) attacks are a **type of network attacks that is relatively simple to conduct**, even for an unskilled attacker.

**They are a major risk as they usually result in some sort of interruption to network services, causing a significant loss of time and money**.

Even operational technologies, hardware or software that controls physical devices or   
 processes in buildings, factories or utility providers, are vulnerable to DoS attacks which can cause a shutdown, in extreme circumstances.

Overwhelming quantity of traffic

This is when a **network, host or application is sent an enormous amount of data at a ate which it cannot handle.**

This causes a **slowdown in transmission or response, or** the device or service to **crash**.

Maliciously formatted packets

A packet is a collection of data that flows between a source and a receiver PC or application over a network, such as the internet.

**When a maliciously formated packet is sent, the receiver will be unable to handle it**.

Attacker forwards packets containing errors or improperly formated packets that cannot be identified by an application, it will cause the receiving device to run very slowly or crash.

Distributed denial of service (DDoS)

**Are similar but originate from multiple coordinated sources.**

1. An attacker builds a network (botnet) of infected hosts (zombies)
2. The zombies computers constantly scan and infect more hosts,
3. When ready, the hacker will instruct the handler system to make the botnet of   
    zombies carry out a DDoS attack

Domain name system

There are many essential technical services needed for a network to operate - such as routing, addressing and domain naming. These are prime targets for attack.

Domain reputation

The **domain name system (DNS) is used by DNS servers to translate a domain name**, such as [www.cisco.com](http://www.cisco.com), into a numerical IP address so that computers can understand it.

If a DNS server does not know an IP address it will ask anotker DNS server.

*An organization needs to monitor its domain reputation, including its IP address, to help protext against malicious external domains*.

DNS spoofing

Or **DNS cache poisoning** is an **attack in which false data is introduced into a DNS resolved cache** - *the temporary database on a computers OS that records recent visits to websites and other internet domains*.

**These poison attacks exploit a weakness in the DNS software that causes the DNS servers to redirect traffic for a specific domain to the attacker’s computer.**

Domain hijacking

When an **attacker wrongfully gains control of a target’s DNS information, they can make unauthorized changes to it**.

This is known as domain hijacking.

This most common way of hijacking a domain name is to *change the administrator’s*  *contact email address through social engineering or by hacking into the administrator’s email account*.

The administrator’s email address can be easily found via the WHOIS record for the domain, which is of public record.

Uniform resource location (URL)

A uniform resource locator (URL) **is a unique identifier for finding a specific resource on the internet**.

Redirecting a URL commonly happens for legitimate purposes.

For example, you have logged into an eLearning portal to begin this cybersecurity essentials course. If you log out of the portal and return to it another time, the portal will redirect you back to the login page.

it is this type of functionality that attackers can exploit. Instead of taking you to the eLearning login page, they can redirect you to a malicious site.

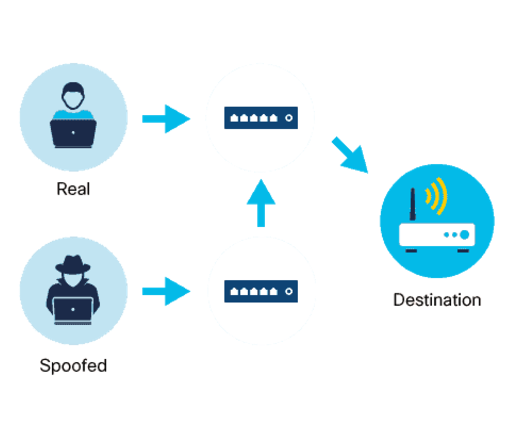
Layer 2 attacks

Layer 2 refers to the data link layer in the open system interconnection (OSI) data communication model.

This layer is used to move data across a linked physical network. IP addresses are mapped to each physical device address (MAC) on the network, using a procedure called address resolution protocol (ARP)

In its simplest terms, the *MAC address identifies the intended receiver of an IP address sent over the network, and ARP resolves IP addresses to MAC addresses for transmitting data*.

Spoofing



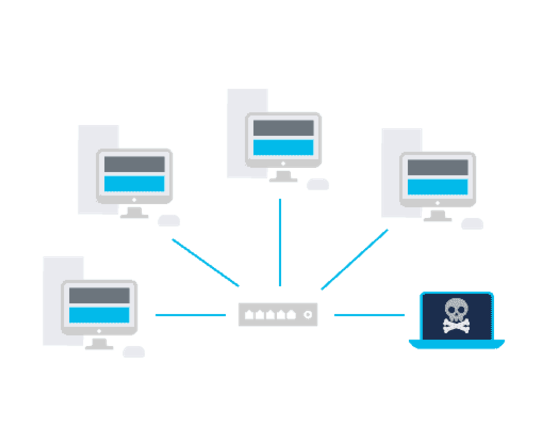
Or poisoning, is a **type of impersonation attack that takes advantage of a trusted relationship between two systems.**

- MAC address spoofing occurs when an **attacker disguises their device as a valid one on the network and can therefore bypass the authentication process.**

- ARP spoofing **sends spoofed ARP msg across a LAN. This links an attacker’s MAC to the IP address of an authorized device on the network.**

- IP spoofing **sends IP packets from a spoofed source address in order to disguise it.**

MAC flooding



Devices on a network are connected via a network switch by using packet switching to receive and forward data to the destination device.

MAC flooding **compromises the data transmitted to a device**. **An attacker floods the network with fake MAC addresses, compromising the security of the network switch**.

Man-in-the-middle and man-in-the-mobile attacks

Attackers can intercept or modify communications between 2 devices to steal info from or to impersonate one of the devices.

Man-in-the-middle

A MitM attack happens when a **cybercriminal takes control of a device without the user’s knowledge**. With this level of access, an *attacker can intercept, manipulate and relay false info between the sender and the intended destination*.

Man-in-the-mobile (MitMo)

Is a **type of attack used to take control over a user’s mobile device**.

**When infected, the mobile device is instructed to exfiltrate user-sensitive info and send it to the attacker**.

Zero-day attacks

**Exploits software vulnerabilities before they become known or before they are disclosed by the software vendor.**

A *network is extremely vulnerable to attack between the time an exploit is discovered and the time it takes for the software vendor to develop and release a patch that fixes this exploit*

Defending against such fast-moving attacks requires network security professionals to adopt a more sophisticated and holistic view of any network architecture.

Keyboard logging

As the name suggests, keyboard logging or keylogging refers to **recording or logging every key struck on a computer’s keyboard.**

Cybercriminals *log keystrokes via software installed on a computer system or* through *hardware devices that are physically attached to a computer*, **and configure the keylogger software to send the log file to the criminal**.

Because it has recorded all keystrokes, this log file can reveal usernames, passwords, websites visited and other sensitive information.