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.

f