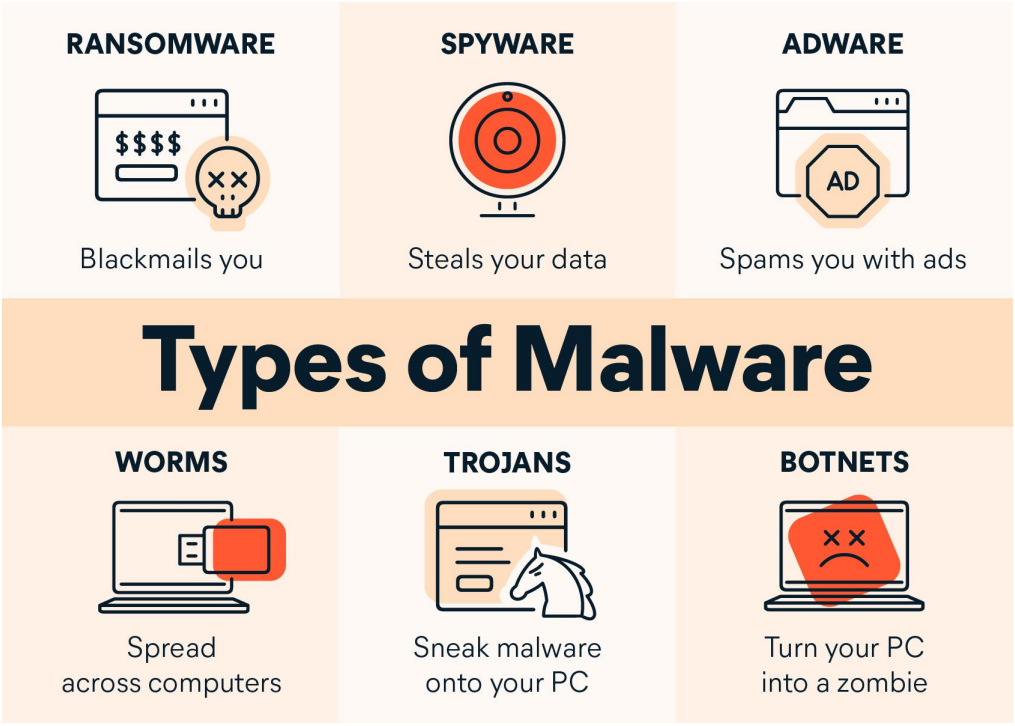
Common Network Security Attacks

Malware

Malware, short for malicious software, refers to any intrusive software developed by cybercriminals (often called hackers) to steal data and damage or destroy computers and computer systems. Examples of common malware include viruses, worms, Trojan viruses, spyware, adware, and ransomware.



Example: Think of malware like a virus in real life. Once someone is "infected," they spread it to others they come into contact with. Similarly, malware can get on your computer and then spread to others connected to your network, potentially harming all infected systems.

What is the intent of malware?

Malware is developed as harmful software that invades or corrupts your computer network. The goal of malware is to cause havoc and steal information or resources for monetary gain or sheer sabotage intent.

Intelligence and intrusion

Exfiltrates data such as emails, plans, and especially sensitive information like passwords.

Disruption and extortion

Locks up networks and PCs, making them unusable. If it holds your computer hostage for financial gain, it's called ransomware.

Destruction or vandalism

Destroys computer systems to damage your network infrastructure.

Steal computer resources

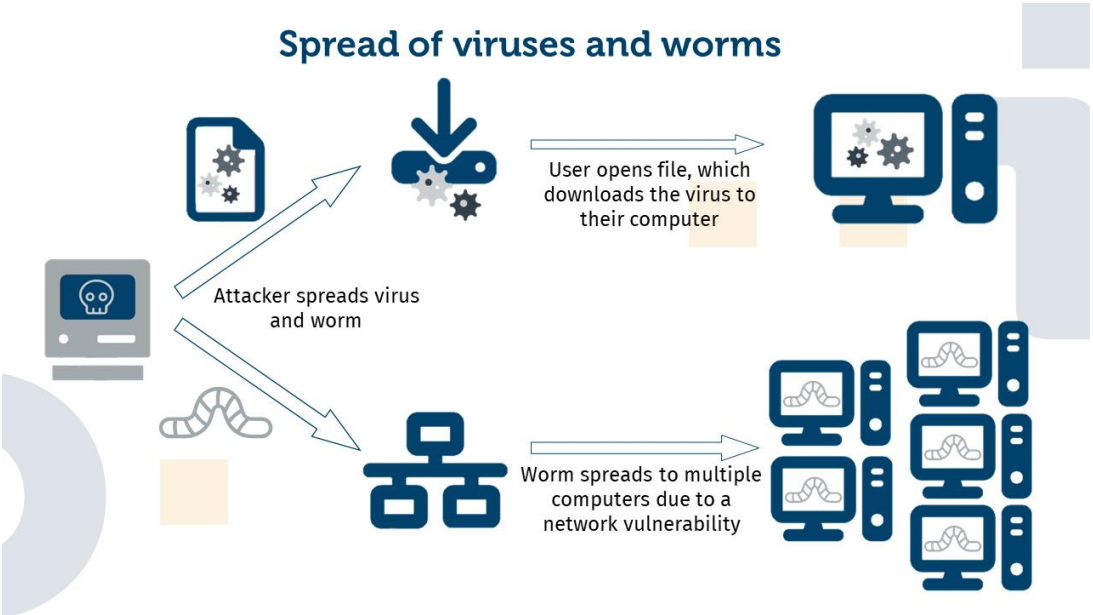
Uses your computing power to run botnets, cryptomining programs (cryptojacking), or send spam emails.

Monetary gain

Sells your organization's intellectual property on the dark web.

Virus

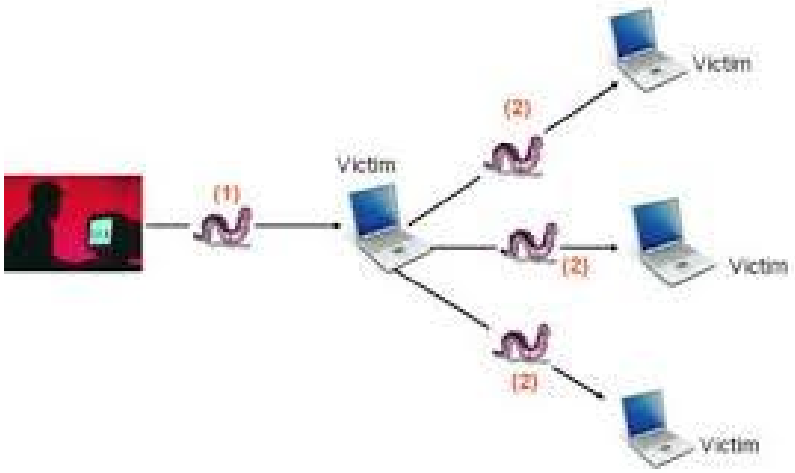
A malware which requires some form of user's interaction to infect the user's device. The classic example is an e-mail attachment containing malicious executable code. If a user receives and opens such an attachment, the user inadvertently runs the malware on the device.



Example: Imagine someone sends you a file titled "Cute Puppies" via email. You open it because it sounds innocent, but it's actually a virus that infects your computer. Now, it can spread to others if you forward the email or share the file.

Worm

A worm is a type of malicious software that rapidly replicates and spreads to any device within the network. Unlike viruses, worms do not need host programs to disseminate. A worm infects a device through a downloaded file or a network connection before it multiplies and disperses at an exponential rate. Like viruses, worms can severely disrupt the operations of a device and cause data loss.



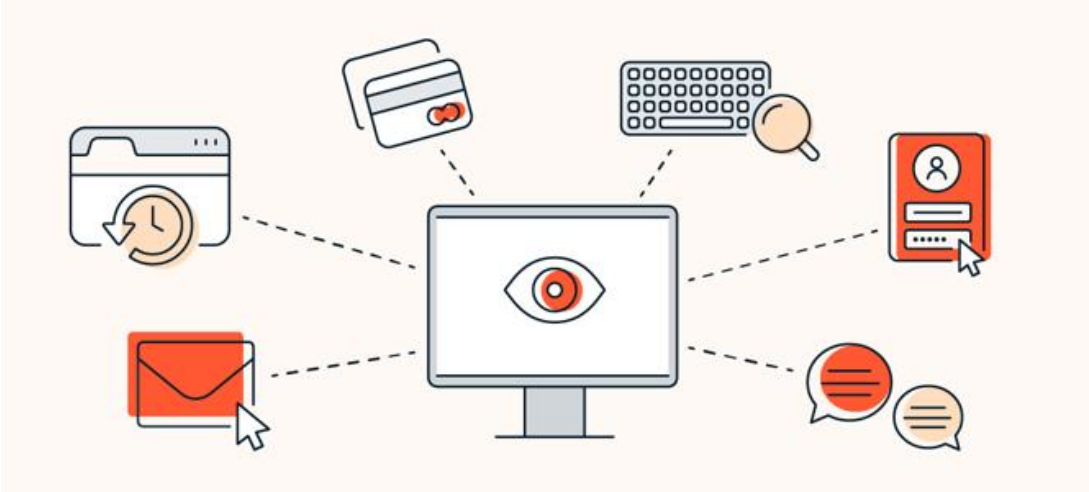
Example: Imagine a worm as a spider crawling from computer to computer without anyone's help. If a network-connected device has a security hole, the worm slips in and starts replicating, moving to other devices on the network without any clicks or actions from users.

Trojan virus

Trojan viruses are disguised as helpful software programs. But once the user downloads it, the Trojan virus can gain access to sensitive data and then modify, block, or delete the data. This can be extremely harmful to the performance of the device. Unlike normal viruses and worms, Trojan viruses are not designed to self-replicate.

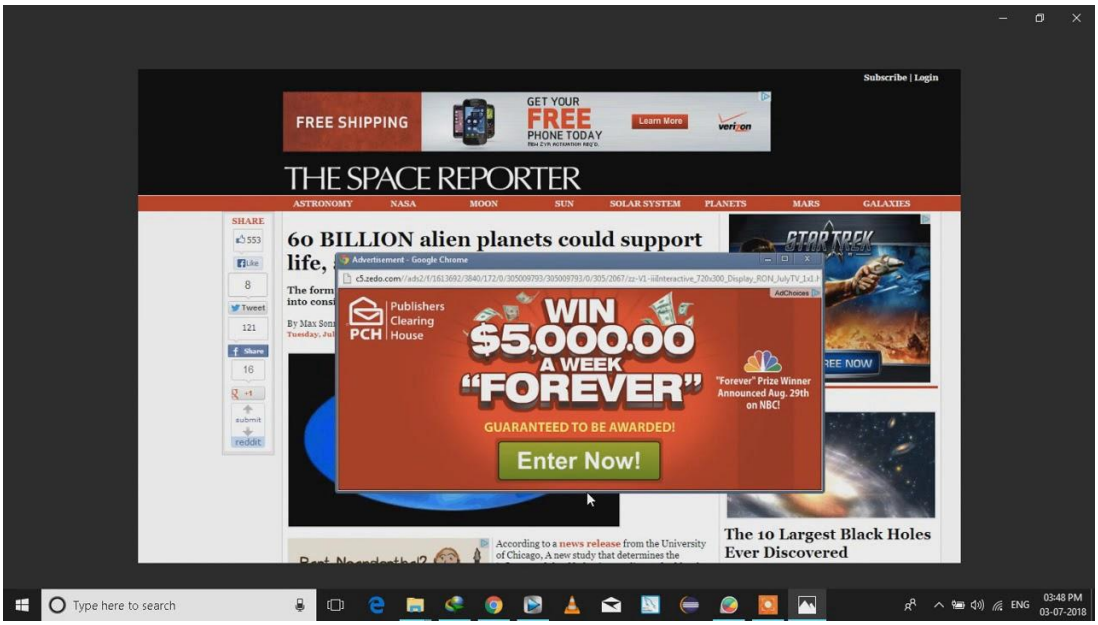
Spyware

Spyware is malicious software that runs secretly on a computer and reports back to a remote user. Rather than simply disrupting a device's operations, spyware targets sensitive information and can grant remote access to predators. Spyware is often used to steal financial or personal information. A specific type of spyware is a keylogger, which records your keystrokes to reveal passwords and personal information.



Adware

Adware is malicious software used to collect data on your computer usage and provide appropriate advertisements to you. While adware is not always dangerous, in some cases adware can cause issues for your system. Adware can redirect your browser to unsafe sites, and it can even contain Trojan horses and spyware. Additionally, significant levels of adware can slow down your system noticeably. Because not all adware is malicious, it is important to have protection that constantly and intelligently scans these programs.



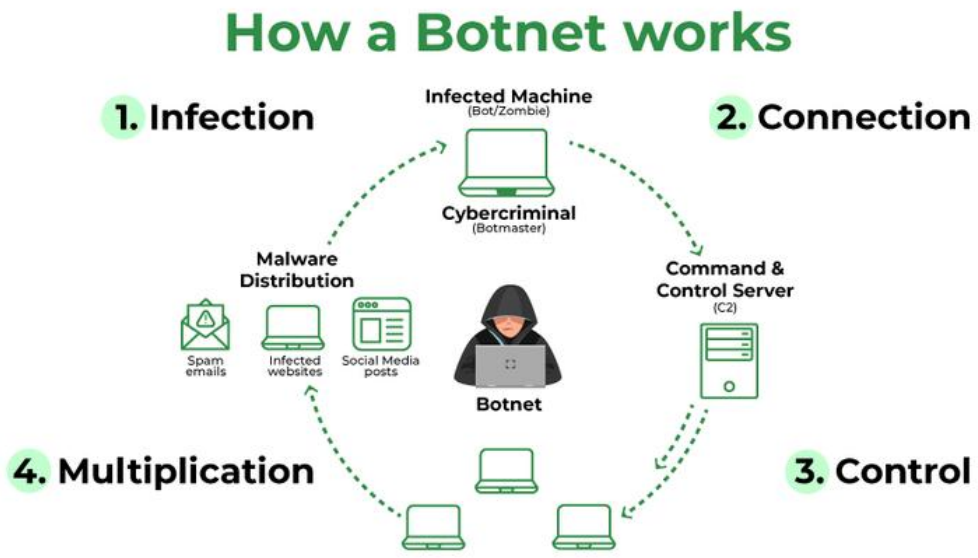
Ransomware

Ransomware is malicious software that gains access to sensitive information within a system, encrypts that information so that the user cannot access it, and then demands a financial payout for the data to be released. Ransomware is commonly part of a phishing scam. By clicking a disguised link, the user downloads the ransomware. The attacker proceeds to encrypt specific information that can only be opened by a

mathematical key they know. When the attacker receives payment, the data is unlocked.

Botnet

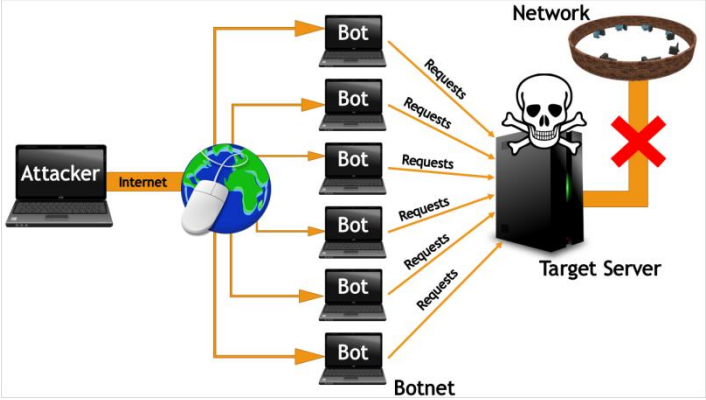
A network of private computers infected with malicious software and controlled as a group without the owners' knowledge, e.g. to send spam.



Example: Picture someone controlling a large group of robots that don't know they're being controlled. A botnet is like that: hackers infect many computers and use them together to send spam or attack websites, without the owners knowing.

DoS (Denial of Service)

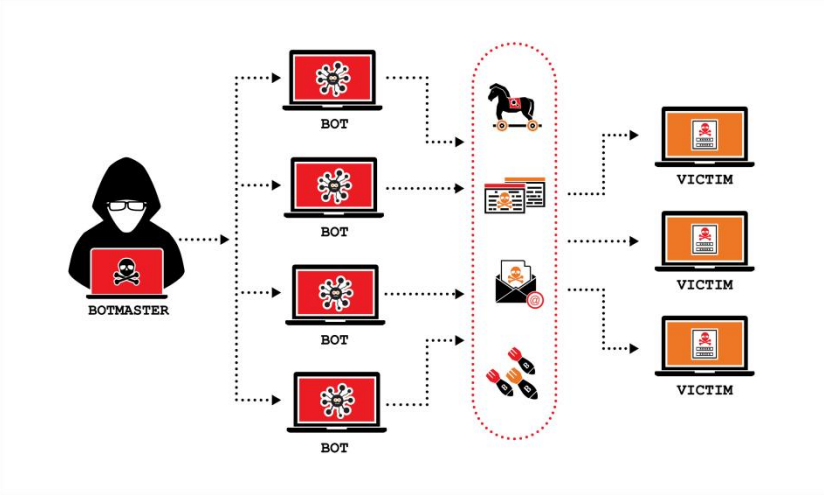
A DoS attack renders a network, host, or other pieces of infrastructure unusable by legitimate users. Most Internet DoS attacks fall into one of three categories :



Example: Imagine a crowd of people standing in front of a store entrance, preventing real customers from entering. In a DoS attack, the attacker floods a website or network with so much traffic that legitimate users can't get in.

DDoS

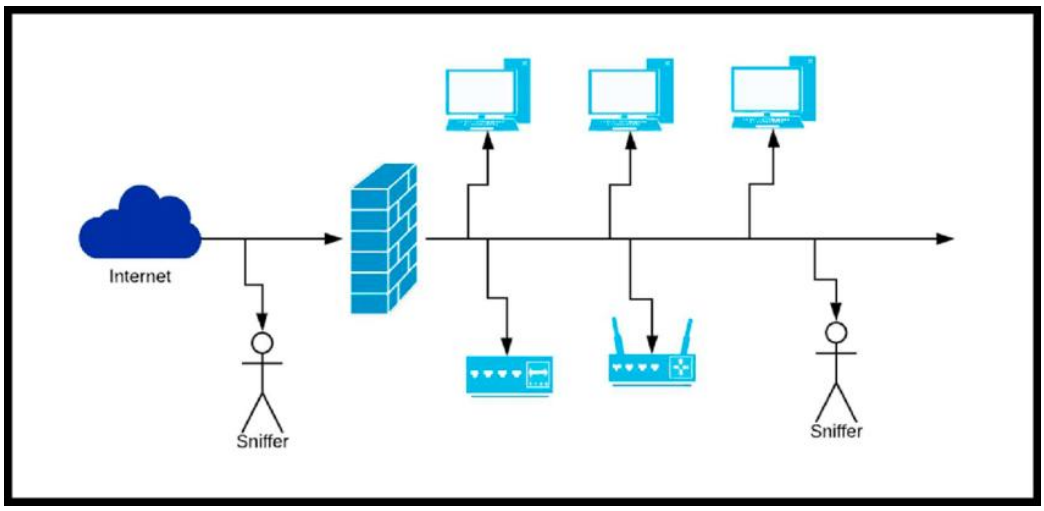
(Distributed Denial of ServiDDoS is a type of DOS attack where multiple compromised systems, are used to target a single system causing a Denial of Service (DoS) attack. DDoS attacks leveraging botnets with thousands of comprised hosts are a common occurrence today. DDoS attacks are much harder to detect and defend against than a DoS attack from a single host. ce)



Example: A DDoS is like hundreds of crowds blocking different entrances to a building at the same time, making it nearly impossible for customers to enter. Attackers use many devices (often botnets) to overwhelm the network, causing it to crash.

Packet Sniffer

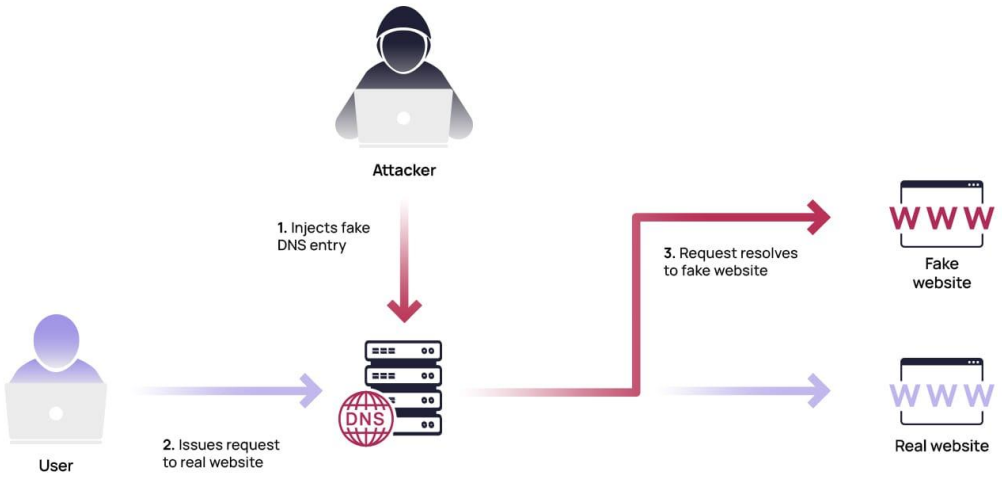
A passive receiver that records a copy of every packet that flies by is called a packet sniffer. By placing a passive receiver in the vicinity of the wireless transmitter, that receiver can obtain a copy of every packet that is transmitted! These packets can contain all kinds of sensitive information, including passwords, social security numbers, trade secrets, and private personal messages. some of the best defenses against packet sniffing involve cryptography.



Example: If you're talking to a friend in a public space, anyone nearby can overhear. Similarly, a packet sniffer can "overhear" unencrypted data being sent over Wi-Fi, potentially capturing private information like passwords.

IP Spoofing

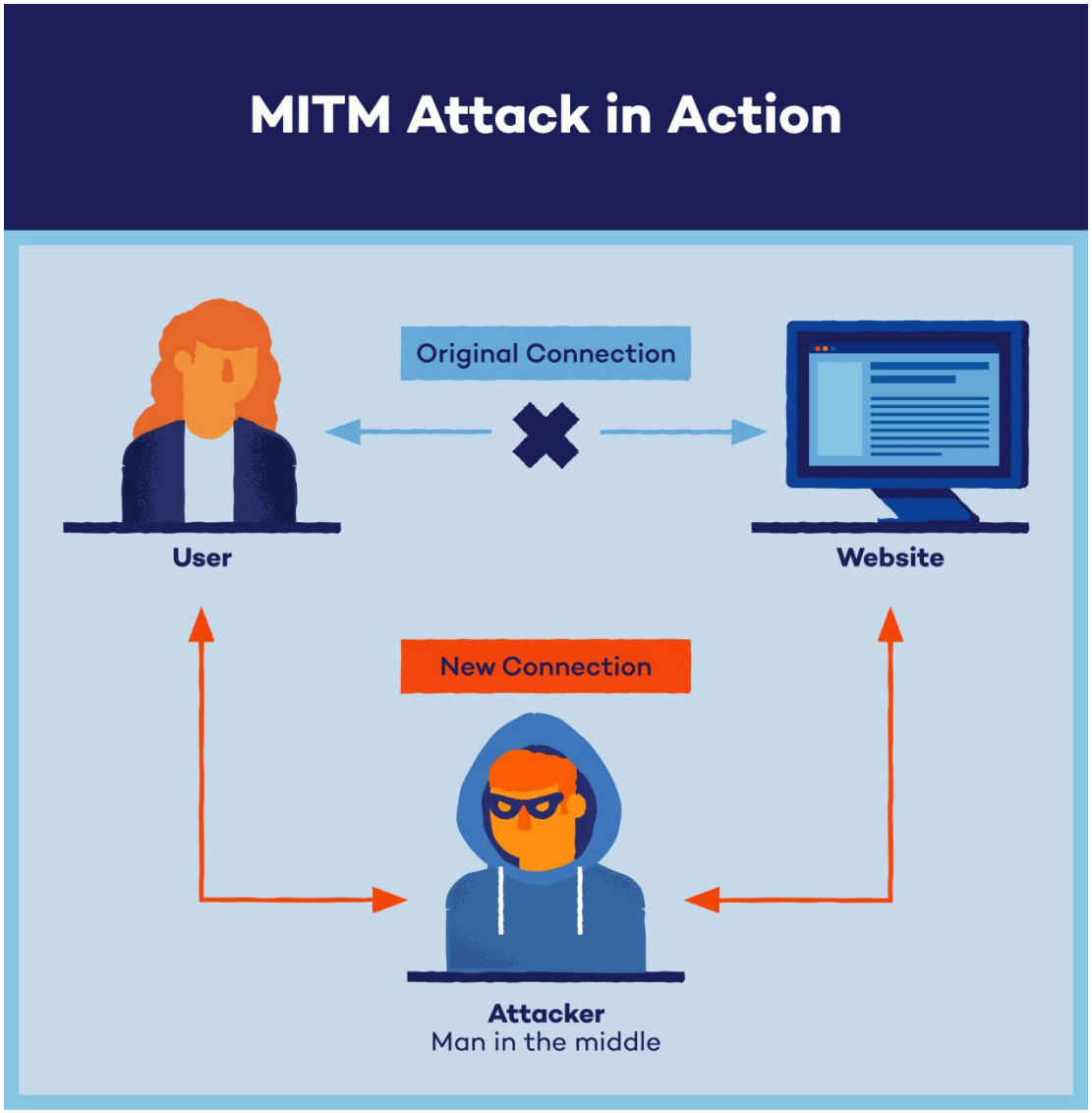
The ability to inject packets into the Internet with a false source address is known as IP spoofing, and is but one of many ways in which one user can masquerade as another user. To solve this problem, we will need end-point authentication, that is, a mechanism that will allow us to determine with certainty if a message originates from where we think it does.



Example: Imagine getting a letter from someone pretending to be your bank. The letter looks official, but it's fake. Similarly, IP spoofing is when attackers disguise their messages to look like they're from a trusted source to trick systems into trusting them.

Man-in-the-Middle Attack

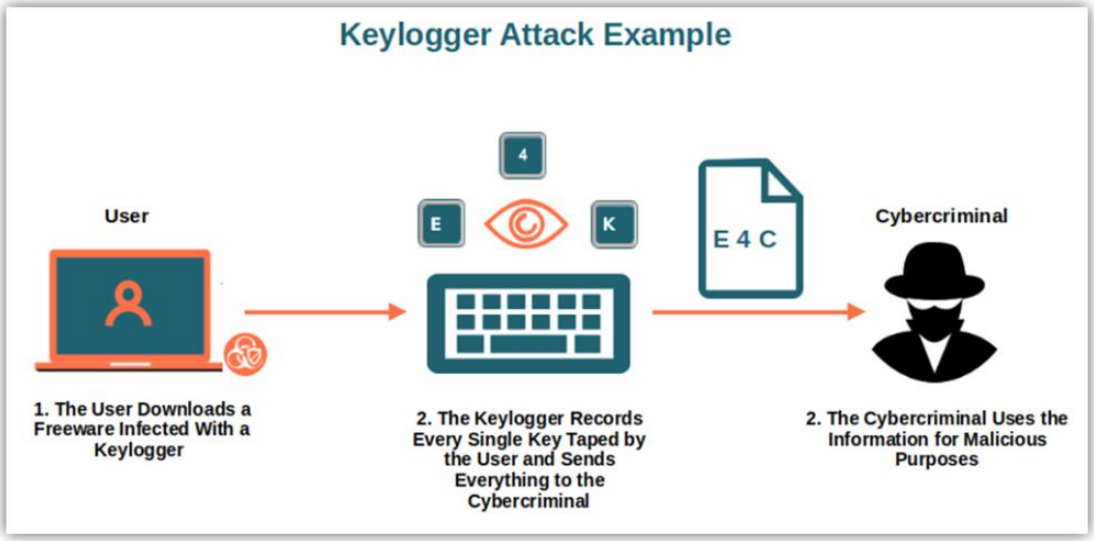
As the name indicates, a man-in-the-middle attack occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. For example, the attacker can re-route a data exchange. When computers are communicating at low levels of the network layer, the computers might not be able to determine with whom they are exchanging data.



Example: Imagine passing a note to a friend, but a sneaky person intercepts the note, reads it, and even changes it before it gets to your friend. A man-in-the-middle attack works similarly, intercepting data between two parties and potentially altering it.

Compromised-Key Attack

A key is a secret code or number necessary to interpret secured information. Although obtaining a key is a difficult and resource-intensive process for an attacker, it is possible. After an attacker obtains a key, that key is referred to as a compromised key. An attacker uses the compromised key to gain access to a secured communication without the sender or receiver being aware of the attack.



Example: Think of a secret code to open a locked box. If a thief somehow steals that code, they can open the box without you knowing. In the same way, if an attacker obtains a key (code) used in encrypted communications, they can read messages without the sender or receiver knowing.

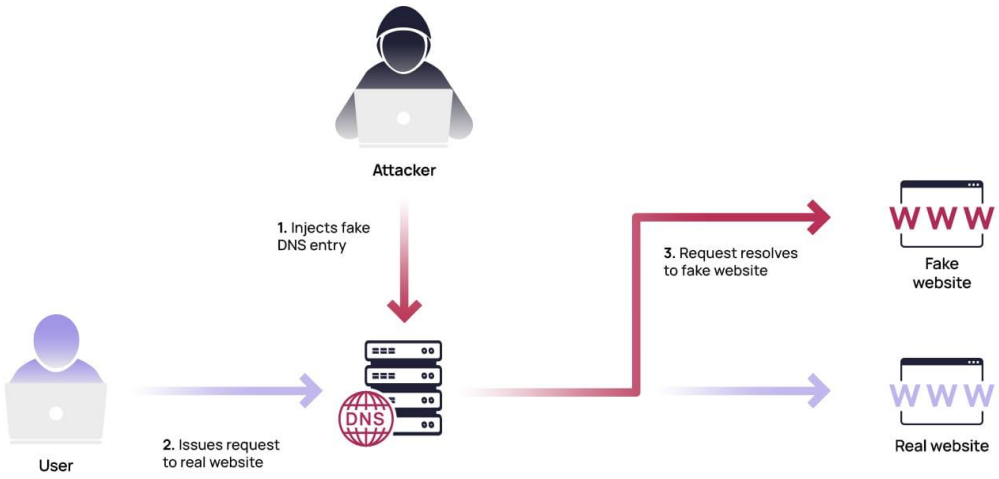
Phishing

The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Example: Imagine someone sends you a message pretending to be your bank, asking for your account details. It looks real, but it's actually a scam designed to steal your information.

DNS Spoofing

Also referred to as DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect IP address.



Example: Suppose you look up the address for a pizza place, but someone hacks the address book, so you get the wrong address and go to a fake pizza place instead. DNS

spoofing works similarly, redirecting users to fake websites to steal information or install malware.

Rootkit

A rootkit is a type of malware that allows cybercriminals to gain access to a computer and remain undetected. Rootkits can be used to:

- Steal sensitive data, such as passwords and credit card information
- Delete files, including operating system code
- Eavesdrop on users
- Install additional malware
- Monitor activities and processes
- Change system configurations
- Execute files

Rootkits are designed to evade detection and can remain hidden for a long time. They can boot up at the same time as the operating system, or even before it.

Some signs of a rootkit include:

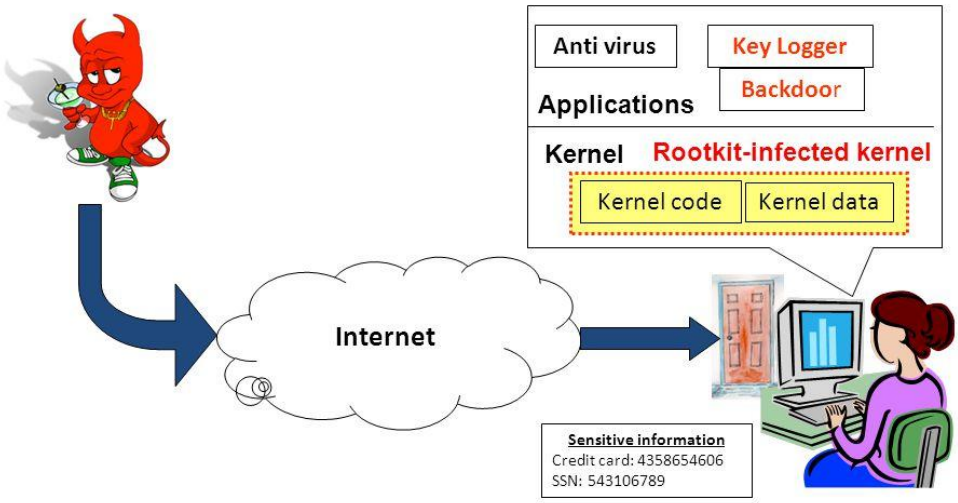
- Blue screen of death
- Unusual web browser behavior, such as unrecognized bookmarks or link redirection
- Slow device performance
- Windows settings change without permission
- Web pages don't function properly

To detect a rootkit, you can run a rootkit scan with your antivirus software. You can also try powering down your computer and running the scan from a clean system.

There are two main types of rootkits: user-mode and kernel-mode. User-mode rootkits are usually easier to detect, while kernel-mode rootkits have access to the core of the operating system

Rootkit-based attack scenario

Rootkits hide malware from anti-malware tools



3

Example: Imagine someone sneaks into your house and hides, so they can spy on you without you noticing. A rootkit is a hidden program that grants attackers “invisible” control over a computer, letting them access files, install malware, or steal data undetected.