Hello everyone! In this video you will learn about malware and its various types.

Malware, is the short form for “malicious software, "It refers to any intrusive software developed by cybercriminals often called “hackers” to steal data and damage or destroy computers and computer systems.

Malware can be detected by observing some common symptoms on your machines. These symptoms may include the slow speed of your computer or web browser over a period of a few days a week, Frequent freezing or crashing of the system, Modified or deleted files, the sudden creation of new programs or desktop icons without your knowledge, programs running and without your consent, Changes in your security settings, Unusual emails/social media messages being sent without your permission, Pop-up advertisements, Browser links redirect to the wrong web page, etc.

The process of malware making its way onto your device is relatively simple: A hacker plans and places a malicious link, file, or attachment in front of their victim, potentially as a phishing email via social engineering tactics. The victim clicks on the infected asset, unknowingly triggering the malware to install onto their device. The malware proceeds to steal, compromise, and/or destroy sensitive data stored on the device.

Common Types of Malware Are Virus, Worms, Trojans, Ransomware, Botnets, Adware, Spyware, Rootkit, Fireless Malware, Malvertising etc.
Let's discuss these malwares one by one.

A virus is malicious software attached to a document or file that supports macros to execute its code and spread from host to host. Once downloaded, the virus will lay dormant until the file is opened and in use. Viruses are designed to disrupt a system's ability to operate. As a result, viruses can cause significant operational issues and data loss.

Worms are a 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 via 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.

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.

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 may or may not be unlocked.

A bot is a software program that performs an automated task without requiring any interaction. A computer with a bot infection can spread the bot to other devices, creating a botnet. This network of bot-compromised machines can then be controlled and used to launch massive attacks by hackers, often without the device owner being aware of its role in the attack.

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.

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 key logger, which records your keystrokes to reveal passwords and personal information.

A rootkit is a type of malware designed to give hackers access to and control over a target device. Although most rootkits affect the software and the operating system, some can also infect your computer's hardware and firmware. Rootkits are adept at concealing their presence, but while they remain hidden, they are active. Once they gain unauthorized access to computers, rootkits enable cybercriminals to steal personal data and financial information, install malware or use computers as part of a botnet to circulate spam and participate in DDoS (distributed denial of service) attacks

File less malware is a type of malicious software that uses legitimate programs to infect a computer. It does not rely on files and leaves no footprint, making it challenging to detect and remove. They use the techniques like exploit kits, memory only malware, stolen credentials etc.

Malvertising (malicious advertising) is the use of online advertising to spread and install malware or redirect your traffic. Cybercriminals inject infected ads into legitimate advertising networks that display ads on websites you

trust. Then, when you visit a site, the malicious ad infects your device with malware — even if you don't click it.

Thank You.