Example of Malware

A Trojan horse, or Trojan, is a type of malicious code or software that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network.

A Trojan acts like a bona fide application or file to trick you. It seeks to deceive you into loading and executing the malware on your device. Once installed, a Trojan can perform the action it was designed for.

A backdoor is a potential security risk.An undocumented way of gaining access to computer system.
Backdoors enable hackers to gain command and control (C&C) of the targeted network without being detected and may use legitimate websites or services to launch an attack. An example of this is to use a web blog URL to decipher the ciphertext and locate any IP addresses of the C&C server list.

A rootkit is a malicious software bundle designed to give unauthorized access to a computer or other software. Rootkits are hard to detect and can conceal their presence within an infected system. Hackers use rootkit malware to remotely access your computer, manipulate it, and steal data.

Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files until a ransom is paid.

Adware is any piece of software, malicious or not, that displays advertisements on a computer. Most often, however, people use the word adware to refer to malicious software that shows deceptive ads, flashing pop-up windows, large banners, and full-screen auto-play commercials within their web browser.

Virus is a specific type of malware that self-replicates by inserting its code into other programs. A virus is a small program designed to cause trouble by gaining access to your device. It can copy your personal data or slow your device down. A virus spreads by replicating and attaching itself to other files.

A worm is a type of malicious software (malware) that replicates while moving across computers, leaving copies of itself in the memory of each computer in its path.

Spyware is malicious software that enters a user's computer, gathers data from the device and user (like passwords, login info, bank account information, credit card numbers, etc.), and sends it to third parties without their consent.

A botnet is a network of computers infected by malware that are under the control of a single attacking party, known as the “bot-herder.” Each individual machine under the control of the bot-herder is known as a bot.

A crypter is a type of software that can encrypt, obfuscate, and manipulate malware, to make it harder to detect by security programs. It is used by cybercriminals to create malware that can bypass security programs by presenting itself as a harmless program until it gets installed.