**Type Of Malware**

1. **Adware**

Often called **advertising-supported software** by its developers, is software that generates revenue for its developer by automatically generating online advertisements in the user interface of the software or on a screen presented to the user during the installation process.

**Behavior** – a lot of pop-up windows and mess with the web browser

1. **Virus**

is a type of malware that, when executed, replicates itself by modifying other computer programs and inserting its own code into those programs. If this replication succeeds, the affected areas are then said to be "infected" with a computer virus.

Computer viruses generally require a host program. The virus writes its own code into the host program. When the program runs, the written virus program is executed first, causing infection and damage. By contrast, a computer worm does not need a host program.

**Behavior** – damaging programs, deleting files, or reformatting the hard drive or replicate themselves or flood a network with traffic and sapping computer memory

1. **Worms**

is a type of malware that can automatically propagate or self-replicate without human interaction, enabling its spread to other computers across a network. A worm often uses the victim organization’s internet or a local area network (LAN) connection to spread itself.

**Behavior** – they may corrupt files, affect communication with other systems, delete files

[**Detect**](https://www.cse.wustl.edu/~jain/cse571-09/ftp/worms/index.html) **-** mistrusted processes

1. **Trojan**

is any malware that misleads users of its true intent by disguising itself as a standard program. he delivery method typically sees an attacker use social engineering to hide malicious code within legitimate software to try and gain users' system access with their software.

[**Behavior**](https://www.fortinet.com/resources/cyberglossary/trojan-horse-virus) – install an .exe to work, spread through emails and files in them, always run when the infected device turns on.

1. **Ransomware**

Is malware that deny user access to files in the infected computer usually demand payment to gain access to them again.

[**Behavior**](https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/) **–** on execute start to work, encrypting data, replace file with encrypt file, delete backups and shadow copies, may add a text file or change background.

1. **Spyware**

Spyware is a malware gather data from the device and user and sends it to third parties usually for profit.

[**Behavior**](https://www.fortinet.com/resources/cyberglossary/spyware) – affect device and network performance, slow down user activity.

1. **Rootkits**

A rootkit is a clandestine computer program designed to gain an admin access to the infect pc without the user notice usually it’s a combination of programs

[**Behavior / Detection**](https://www.kaspersky.com/resource-center/definitions/what-is-rootkit) – a large volume of windows error messages or blue screen, unusual web browser behavior, slow performance, settings changes.