Malware

AGENDA

➢ Definition
➢ Malware Types
➢ Virus
➢ Trojan
➢ Worm
➢ Spyware
➢ Keylogger
➢ Ransomware
➢ RootKit
➢ How machines get infected with malware

Malware Definition

Stands for Malicious Software, a Piece of software that developed by the malicious Actor to damage, or gain unauthorized access to the Victim machine.

Malware Types (1)

Virus: is a standalone malicious software not embedded in another program, the user must click on the virus executable itself.

Trojan: a malware that is often disguised as a legitimate file, the attacker embedded the malicious code inside the file, Hence the file will appear to the User as a usual file to encourage the user to open the file, and in the background is malicious software.

twinkl.com
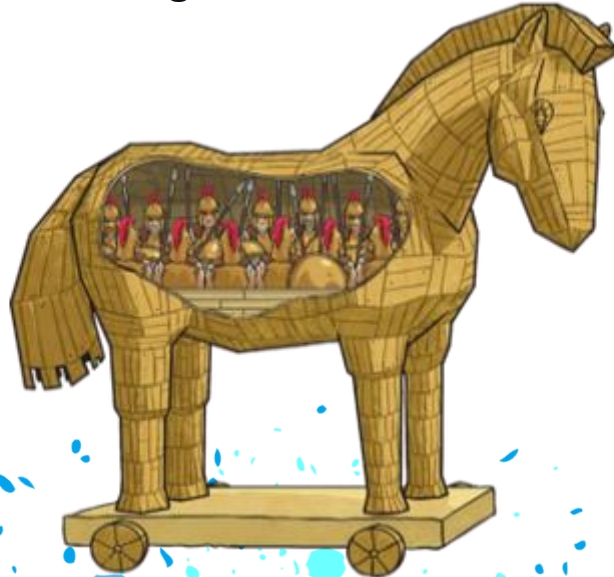
Malware Types (2)

Worm: is a self-replicating malicious Software that can spread throughout a network without human assistance by exploiting vulnerabilities in Software and Operation systems

Spyware: is a malicious Software that gathers information about you, including the sites you visit, the things you download, your usernames and passwords, payment information, and the emails you send and receive.

Keylogger: a kind of spyware that record and steal keystrokes that user enters.

Malware Types (3)

Ransomware: is a malicious software that steal and Encrypt that sensitive files on the victim machine and then ask pop-up a ransom message for money transfer.

Rootkits: a malicious software that designed to remain hidden on the victim machine, rootkit required an admin privilege to be installed on the victim machine.

How machines get infected with malware?

1. Phishing emails.
2. Infected removable drives.
3. Bundled with other software.
4. Hacked or compromised webpages.
5. Other malware

Thanks!

Any questions?