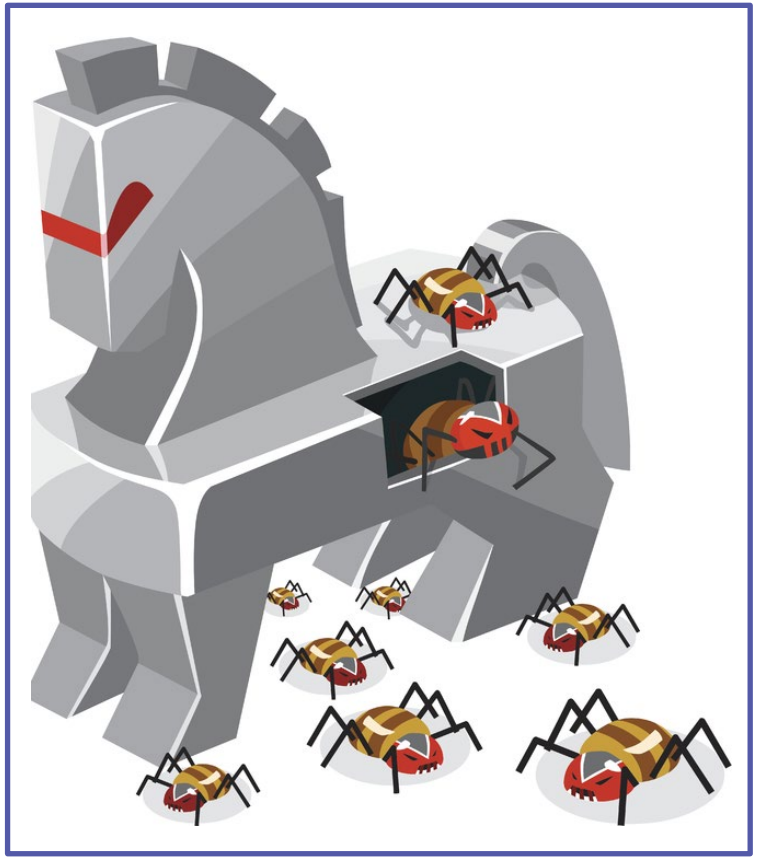
Cybersecurity

2.4.3 - Trojans, Backdoors, and RATs

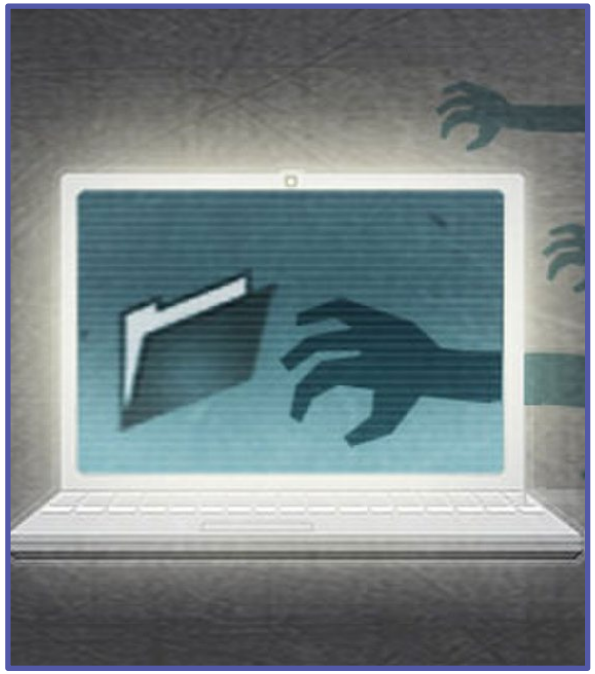
Trojans

- Software that is downloaded, installed, and seems harmless but does have a malicious intent
- Reference to the Greek story of the siege of Troy
- Unlike typical viruses, trojans cannot self-replicate nor propagate without user interaction
- In most cases a user falls victim to a social engineering scheme and downloads the software thinking it is a harmless attachment or something they need or want.



Backdoors

- The ability to access a system or data by bypassing the security controls
- Avoids the normal login process
- Can occur through various means
  - Malware might install a backdoor to get back into the system
  - Software may contain accidental backdoors meant originally to perform maintenance
  - There could be an exploit that allow an intruder to gain access through a backdoor



Remote Access Trojans (RAT)

- A type of trojan that combines the use of a backdoor allowing a malicious actor to have administrative and remote control of the host
- Allows a hacker to connect remotely and examine files, log keystrokes, find passwords, take screenshots, or use the connection to download additional malware

Other Forms of Trojans

- Downloader Trojans can imitate pre-existing software that may need an update or serve to update pre-existing malware already installed on the device.
- DDoS Trojans infect a victim's computers then perform DDoS attacks in hopes of disrupting network services
- SMS Trojans can infect mobile devices and send and intercept messages

Trojan Defense

- Never download or run unknown or untrusted software
- Verify signatures or hashes from developers prior to installing software
- Keep anti-virus software updated
- Back-up important files in the event a trojan is installed
- Be mindful of opening attachments, even from known senders