Malware Notes

Table of contents

Anish Goyal   Schepens   Period 1   01/24/2023

Trojan horses

- Do exactly what they say plus something bad
- "Trick" the user into running itself through an innocuous-looking program

Viruses

- Modify a program to do something bad
- Can be spread by email, floppy disks, etc.
- Wraps some part of the code at the start of the program (initialization) and the back of the program

Malware

- Independent malware

  - Trojan horses do not need a host because they are something that can run and sustain themselves (this is debatable)
  - Worms and bots
    * Worms will try to copy themselves to other computers on the same LAN or WAN
    * A bot or a zombie is a computer that is infected with a worm or backdoor and is controlled by a hacker
    * Bot code (malware) on the computer communicates with the attacker's server and carries out malicies activities per attacker's instructions
    * Botnet is a network of computers that are infected with a bot or a worm
      · Typically used to carry out DDoS attacks

- Dependent malware

  - Viruses need a host because they are a part of a program, while trojan horses are their own host