CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Malicious Software and Denial of service attacks

Introduction to Malicious software

Video Summary

- What is Malware
- Attack Sources
- Attack Kits
- Classification of Malware
- Malware Symptoms

Malware

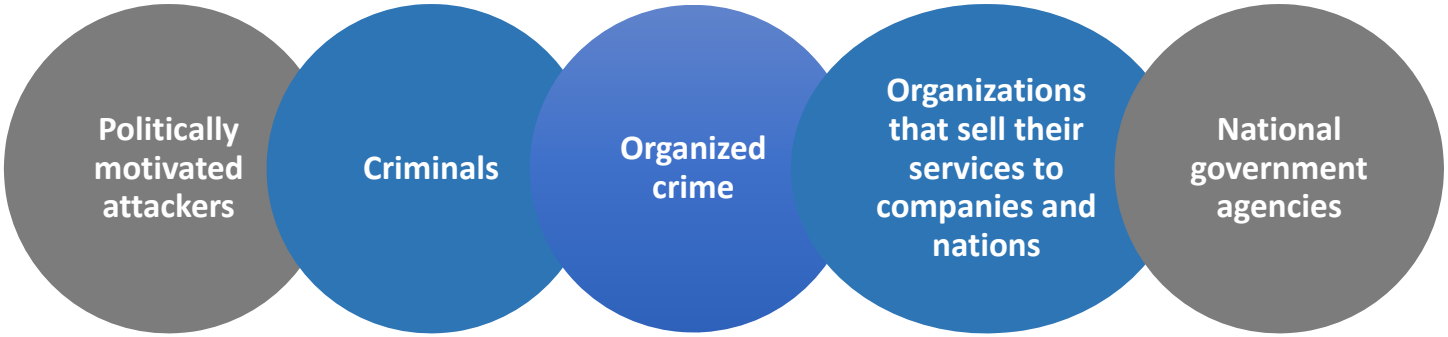
NIST 800-83 defines malware as:

"a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim."

Unwanted software that doe something bad: damages systems, steals information, consumes resources, extorts money, forcibly displays advertising, etc.

Attack Sources

- Another significant malware development is the change from attackers being individuals often motivated to demonstrate their technical competence to their peers to more organized and dangerous attack sources such as:



- This has significantly changed the resources available and motivation behind the rise of malware and has led to development of a large underground economy involving the sale of attack kits, access to compromised hosts, and to stolen information

Attack Kits

- Initially the development and deployment of malware required considerable technical skill by software authors
  - The development of virus-creation toolkits in the early 1990s and then more general attack kits in the 2000s greatly assisted in the development and deployment of malware
- Toolkits are often known as “crimeware”
  - Include a variety of propagation mechanisms and payload modules that even novices can deploy
  - Variants that can be generated by attackers using these toolkits creates a significant problem for those defending systems against them
- Examples are:
  - Zeus
  - Angler

Classification of Malware

Classified into two broad categories:

- Based first on how it spreads or propagates to reach the desired targets
- Then on the actions or payloads it performs once a target is reached

Also classified by:

- Those that need a host program (parasitic code such as viruses)
- Those that are independent, self-contained programs (worms, trojans, and bots)
- Malware that does not replicate (trojans and spam e-mail)
- Malware that does replicate (viruses and worms)

Malicious Software

- A classification of malware:

  Propagation how the malware spreads
  - Viruses
  - Worms
  - Social engineering

  Payload actions malware takes when reaches victim
  - System corruption
  - Zombies and bots
  - Information theft
  - Stealthing

- Countermeasures: anti-virus software

Malware By Propagation Techniques

- How it moves from one computer to another?
  - Download a file (malicious file)
  - Found a flash drive ➔ Insert to your computer ➔ Infect your files
  - Email ➔ attachment from unknown source

Network

Virus

Spreads via “hosts” (such as programs, scripts, Web apps) like biological virus

Modifies code without consent

Human actions cause spreading of virus

Early occurrence: “Elk Cloner”
(Apple II boot sector virus, 1982)

Worm

Self-replicating malware

Example: spread via e-mail transmission

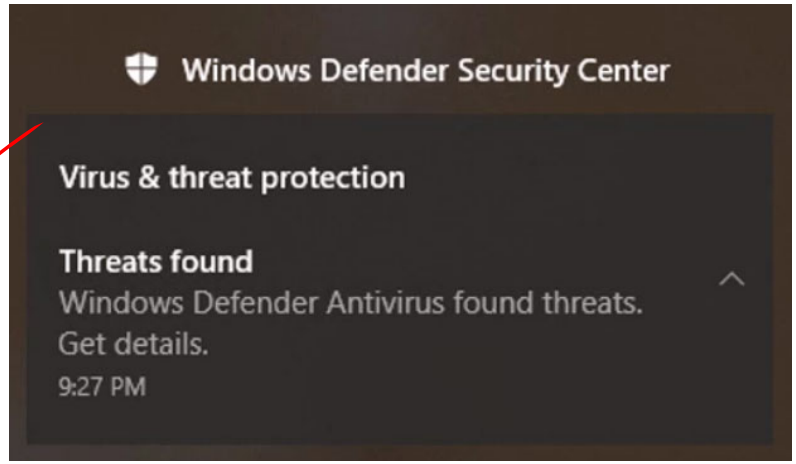
Can consume system/network bandwidth

Standalone program (unlike a virus)

Early occurrence: Blaster worm (2003)

Malware Symptoms

- Unexpected behavior
- GUI changes (such as icon color)
- Browser goes to wrong page
- Contacts receive emails from you that you didn't send
- Slow boots and logins



Video Summary

- What is Malware
- Attack Sources
- Attack Kits
- Classification of Malware
- Malware Symptoms