CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Malicious Software and Denial of service attacks

Other Malwares and Countermeasures

Video Summary

- Other types of Malwares
- Zombies and Bots
- Information Theft
- System Corruptions
- Countermeasures

Ransomware

Restricts user access to data and/or programs

"crypto ransomware"

"locker ransomware"

May (or may not) decrypt files once ransom is paid, often in cryptocurrency

Early occurrence: PC CYBORG (1989)

WannaCry

SMB: Server Message Block

Rootkit

Malware with stealth features ("cloaking")

Hard to detect and remove

Can run before OS loads

Can have privileged ("root") access

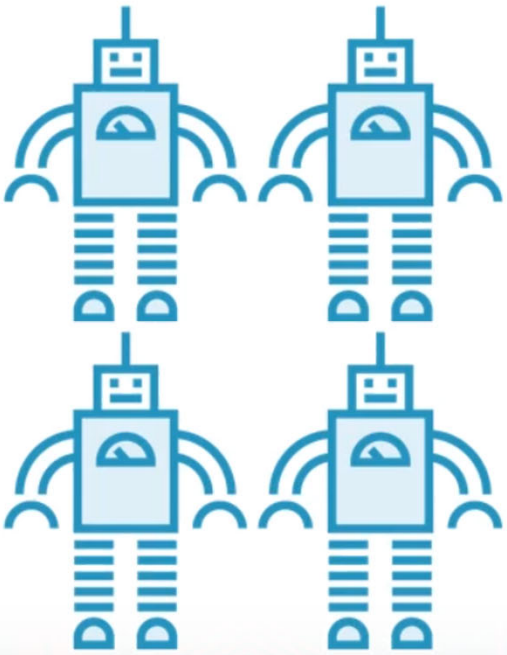
Early occurrences: NTRootkit (1999), Sony DRM (2005)

UEFI Secure Boot

Windows

- UEFI ensures boot loader is properly signed. If not, will not boot
- Helps prevent rootkits from replacing boot loader
- Can be turned off by anyone with admin access to UEFI settings

Botnet of Zombies



"Botnet" = Robot network

"Zombie" = computer under external control

Controlled by single entity

- Possibly for spam...
- ...or DDoS attacks

Typically includes stealth features

Early occurrence: Earthlink spammer (2000)

Zombies and Bots

- Uses:
  - ✓ Distributed DoS attacks
  - ✓ Spamming
  - ✓ Sniffing traffic
  - ✓ Keylogging
  - ✓ Spreading new malware
  - ✓ Installing advertisement add-ons and browser plugins

Information Theft

Keyloggers

- Captures keystrokes to allow attacker to monitor sensitive information
- Typically uses some form of filtering mechanism that only returns information close to keywords, e.g. "login", "password"

Spyware

- Subverts the compromised machine to allow monitoring of a wide range of activity on the system
- Monitoring history and content of browsing activity
- Redirecting certain Web page requests to fake sites
- Dynamically modifying data exchanged between the browser and certain Web sites of interest

May be legal (ex: ad-targeting)

System Corruption

- Action taken by malware on system: corrupt the system

- Data Destruction:
  - ✓ Delete data
  - ✓ Overwrite data
  - ✓ Encrypt data and then demand payment (ransomware)
- Real-World Damage:
  - ✓ Corrupt BIOS code so computer cannot boot
  - ✓ Control industrial systems to operate such that they fail (Stuxnet worm)
- Logic Bomb
  - ✓ Activate when certain conditions are met (date = time)

Countermeasures

Malware Countermeasure Approaches

- Prevention is an ideal solution, but almost impossible
  - ✓ Elements of prevention: policy, awareness, vulnerability mitigation, threat mitigation
  - ✓ Ensure systems are up-to-date (fix all bugs)
  - ✓ Apply Access Control (no permissions for malicious software to access files)
  - ✓ User awareness and training
- Detection, identification and removal (antivirus)
  - ✓ Generality
  - ✓ Timeliness
  - ✓ Resiliency (the antivirus can protect itself)
  - ✓ Global and local (your computer and the organization servers)
  - ✓ Transparent (antivirus shouldn't hide what it is doing)

User Education

- Know how to read e-mail headers
- Know how to check suspicious links
- Never provide credentials via email
- Never download unknown attachments

Generic Decryption

- A polymorphic virus must decrypt itself to activate
- Generic decryption runs executable code in virtual machine, monitors instructions
  - ✓ CPU emulator: virtual machine software
  - ✓ Virus signature scanner: scans for signatures
  - ✓ Emulation control module: monitors and controls execution of target code
- If decryption performed, malware is exposed and detected
- How long to run each anti-virus scan?
  - ✓ Too long: system performance degraded
  - ✓ Too short: do not see most of malware

Development of Anti-virus Software

- 1st generation: simple scanners
  - ✓ Requires a malware signature to identify the malware
  - ✓ Limited to the detection of known malware
- 2nd generation: heuristic scanners
  - ✓ Uses heuristic rules to search for probable malware instances
  - ✓ Another approach is integrity checking
- 3rd generation: activity traps
  - ✓ Memory-resident programs that identify malware by its actions rather than its structure in an infected program
- 4th generation: full featured protection
  - ✓ Packages consisting of a variety of anti-virus techniques used in conjunction
  - ✓ Include scanning and activity trap components and access control capability

Realtime Monitoring Softwares

This software wants to access “certain feature” do you want to allow it?

- Integrates with OS, monitors program behavior in real-time
- Block potentially malicious actions before they affect system
  - ✓ Attempts to open, view, delete, modify files
  - ✓ Attempts to format disks
  - ✓ Modifications to logic of executable files
  - ✓ Modification of critical system settings
  - ✓ Scripting of email to send executable files
  - ✓ Initiation of network connections

Antimalware Programs

Windows Defender comes with Windows 10

macOS does *not* include antimalware GUI

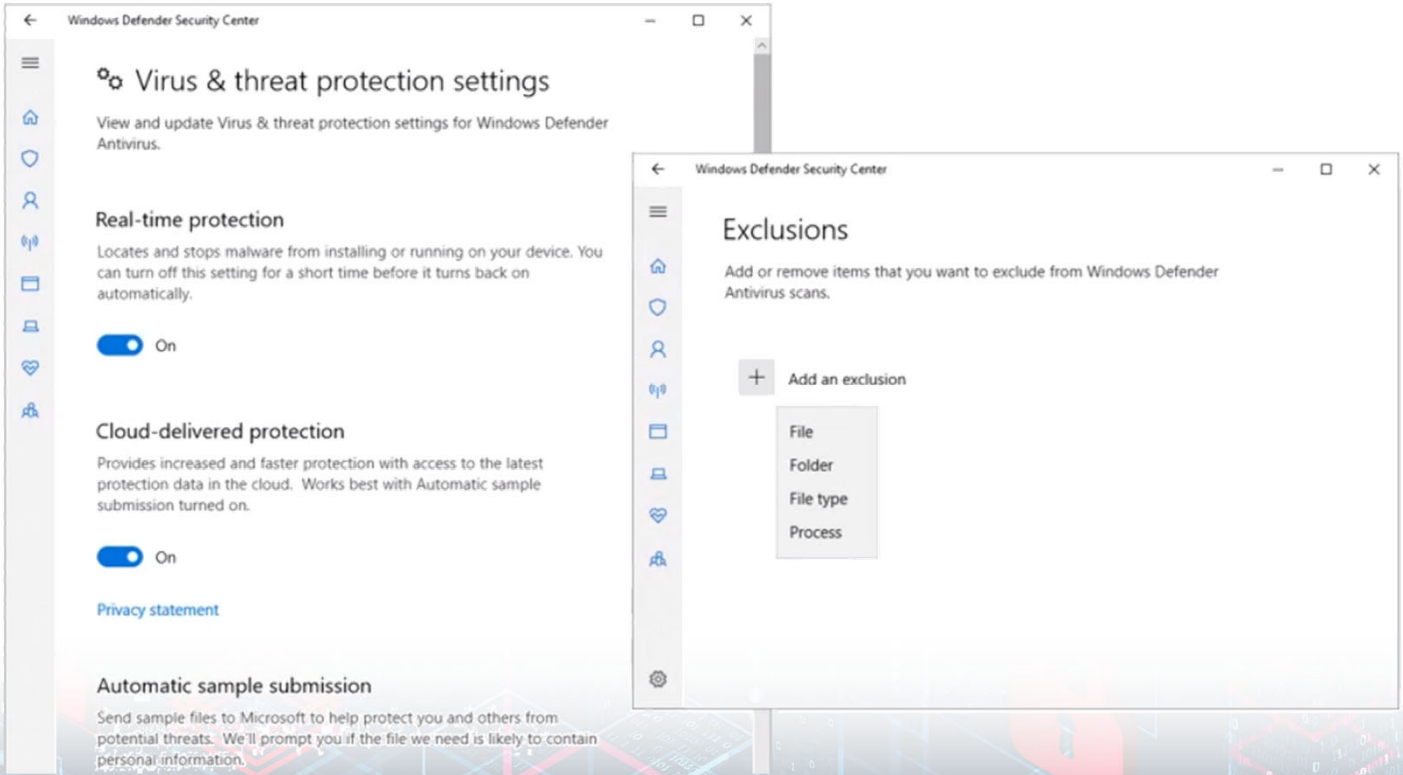
Features to look for:

- Real-time protection
- Ad-hoc scanning
- Periodic deep scans
- Offline scanning
- Light impact on OS
- Reputation databases

Windows Security

https://app.pluralsight.com/

Windows Defender Settings



https://app.pluralsight.com/

Video Summary

- Other types of Malwares
- Zombies and Bots
- Information Theft
- System Corruptions
- Countermeasures