1213 سبر

Network Defense

Lecture #6 Part 1

Comparing Threats, Vulnerabilities, and Common Attacks

جامعة الملك سعود
King Saud University

Topics

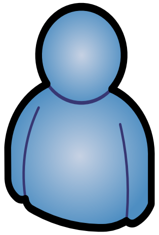
1. **Understanding Threat Actors**
2. **Determining Malware Types**
3. **Recognizing Common Attacks**
4. **Blocking Malware and Other Attacks**

Threat Actors

- Hacker
  - Malicious individuals who use their technical expertise to launch attacks
- Script kiddie
  - Little expertise, sophistication, or funding
- Hacktivist
  - Part of an activist movement
- Insider
  - Employee (can become a malicious insider)

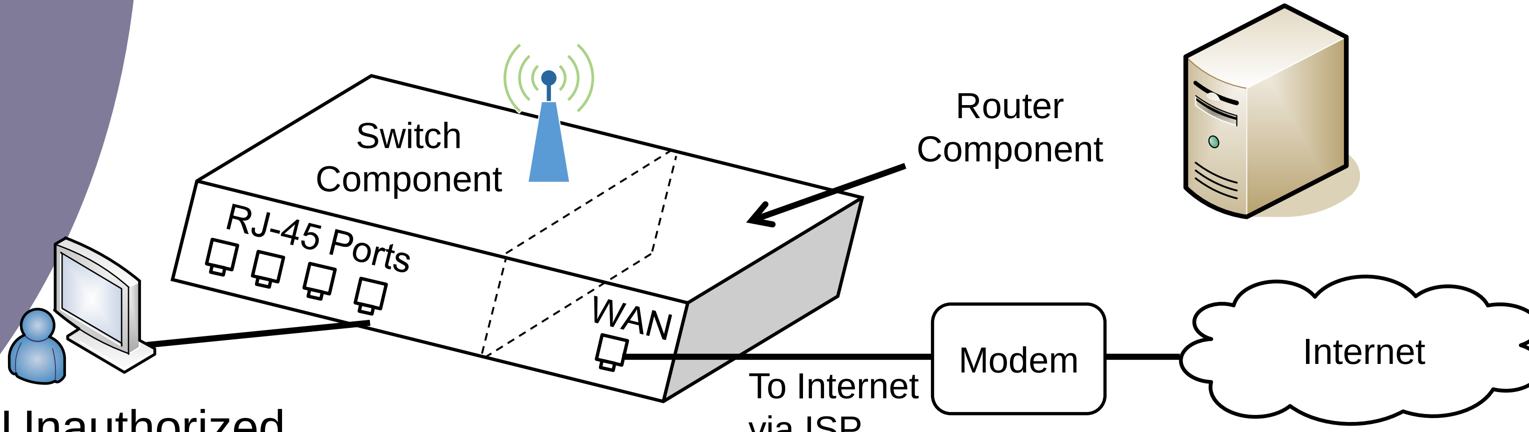
Threat Actors

- Nation state/advanced persistent threat (APT)
  - Identify a target and persistently attack until they gain access
  - Often remain in network for months or years
  - China PLA Unit 61398
  - Russia APT 28 (Fancy Bear)
  - Russia APT 29 (Cozy Bear)



Threat Actors

- Attack vectors
  - Email
  - Social media
- Shadow IT



Unauthorized Server

Router Component

Switch Component

RJ-45 Ports

WAN

To Internet via ISP

Modem

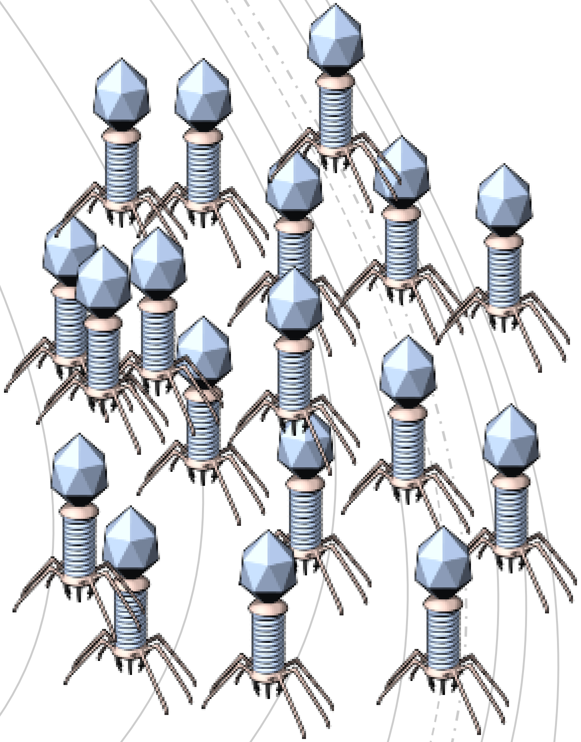
Internet

Unauthorized Access Point

Determining Malware Types

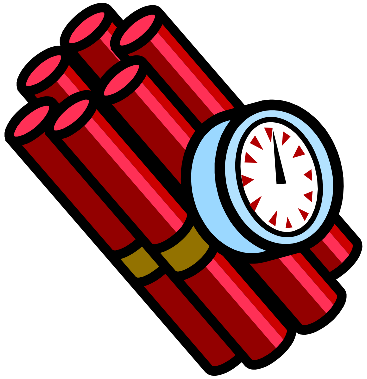
Viruses

- **Replication mechanism**
- **Activation mechanism**
- **Payload mechanism**



Determining Malware Types

- **Worms**
  - **Self replicating**
- **Logic bombs**
  - **Executes in response to an event**
- **Backdoors**
  - **Provides an alternate method of access**
  - **Many types of malware create backdoors**



Determining Malware Types

- **Trojan Horse**
  - **Appears to be useful but is malicious**
  - **Pirated software, rogueware, or games**
  - **Also infect systems via USB drives**
- **Drive-by downloads**
  1. **Attackers compromise a web site to gain control of it**
  1. **Attackers install a Trojan embedded in the web site's code**
  1. **Attackers attempt to trick users into visiting the site**
  1. **When users visit, the web site attempts to download the Trojan onto the users' systems**
- **Remote access Trojan (RAT)**

Determining Malware Types

- Keylogger
  - Capture’s keystrokes
- Spyware
  - Can access a user’s private data and
    result in loss of confidentiality

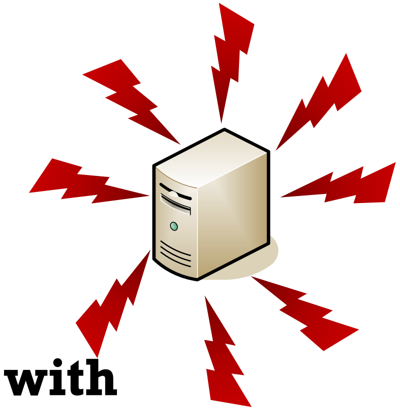
Determining Malware Types

- Rootkits
  - System level or kernel access
  - Can modify system files and system access
  - Hide their running processes to avoid detection with hooking techniques
  - File integrity checker can detect modified files
  - Inspection of RAM can discover hooked processes

Bots and Botnets

- Bots – software robots

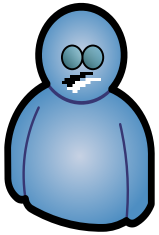
- Botnets
  - Controlled by criminals (bot herders)
  - Manage command and control centers
  - Malware joins computers to robotic network



- Zombies or clones
  - Computers within botnet
  - Join after becoming infected with malware

Determining Malware Types

- Ransomware
  - Takes control of user's system
  - Typically encrypts user's data
  - Attempts to extort payment



We have your data
Pay up or you'll never see it again

Determining Malware Types

- Potentially unwanted programs (PUPs)
  - Legitimate, but some are malicious, such as Trojans
- Fileless virus
  - Memory code injection
  - Script-based techniques
  - Windows Registry manipulation

Social Engineering

- Flattery and conning
- Assuming a position of authority
- Encouraging someone to:
  - Perform a risky action
  - Reveal sensitive information
- Impersonating
- Tailgating