

# Types of Security Attacks

- ▶ Reconnaissance Attack
- ▶ Access Attack
- ▶ DoS / DDoS
- ▶ Malicious Code Attack

```
mirror_mod = modifier_obj
# set mirror object to mirror
mirror_mod.mirror_object = mirror_obj
# set mirror object to mirror
mirror_mod.mirror_object = mirror_obj

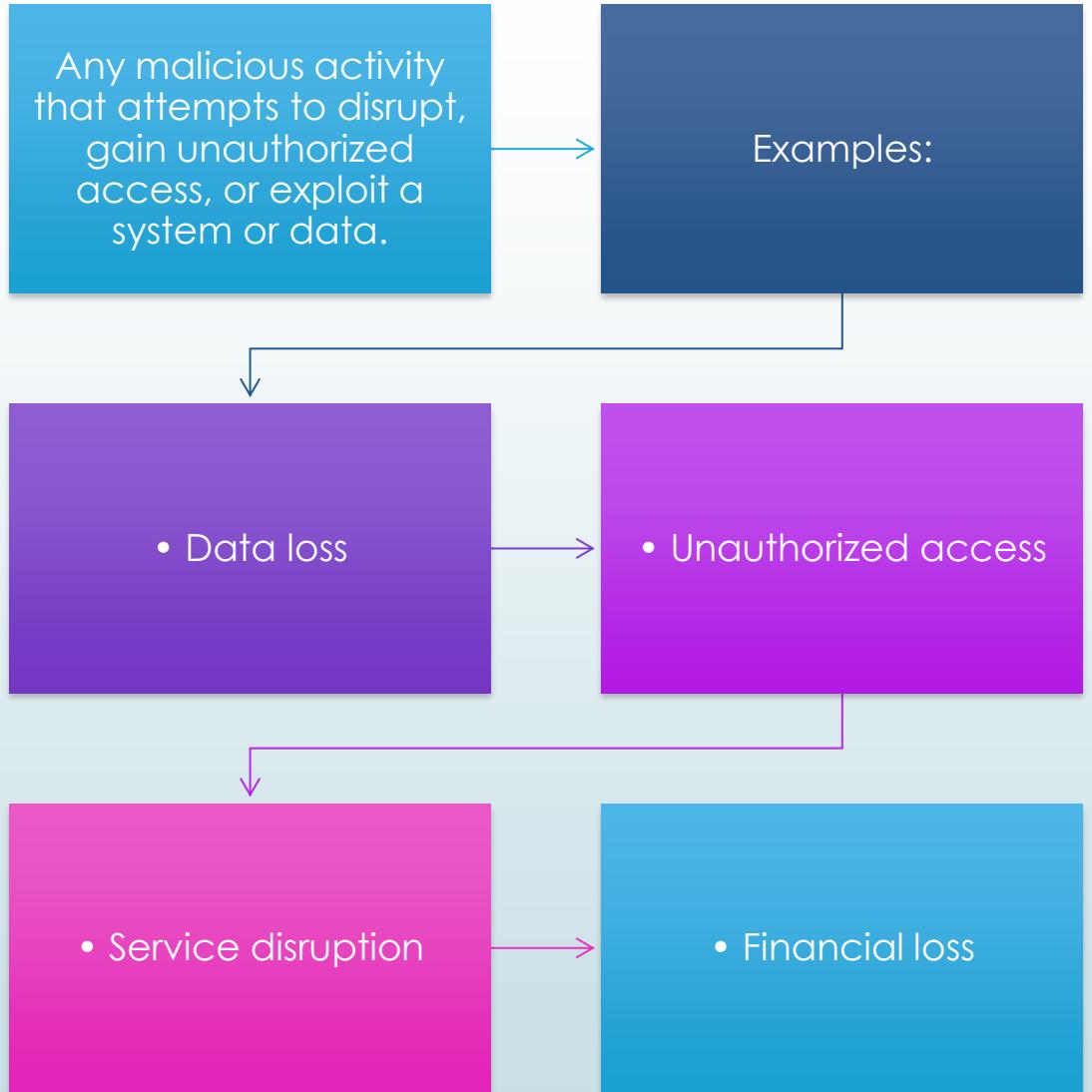
mirror_mod.use_x = False
mirror_mod.use_y = True
mirror_mod.use_z = False
if operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

# selection at the end - add
# mirror_ob.select= 1
# mirror_ob.select=1
context.scene.objects.active = eval("Selected" + str(modifier))
mirror_ob.select = 0
bpy.context.selected_objects.append(mirror_obj)
data.objects[one.name].select = 1
print("please select exactly one object")
print("operator created")

- - - - - OPERATOR CLASSES - - - - -
```

```
types.Operator):
    X mirror to the selected
    object.mirror_mirror_x"
    for X"
    context):
    context.active_object is not
```

# What is a Security Attack?





## Reconnaissance Attack

- ▶ Definition: Gathering information about the target.
- ▶ Techniques:
  - ▶ • Port scanning (Nmap)
  - ▶ • Banner grabbing
  - ▶ • SNMP walk
  - ▶ • Social engineering



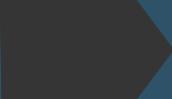
## Reconnaissance Scenario & Prevention

- ▶ Example: Hacker uses Nmap to scan open ports on a company web server.
- ▶ Prevention:
  - ▶ • Firewall rules
  - ▶ • IDS/IPS detection
  - ▶ • Disable unused services



## Access Attack

- ▶ Definition: Attempt to gain unauthorized access.
- ▶ Examples:
  - ▶ • Brute-force / password guessing
  - ▶ • Privilege escalation
  - ▶ • Exploiting unpatched systems
  - ▶ • SQL injection



# Access Attack Scenario & Defense

- ▶ Scenario: Attacker uses leaked credentials to log in and escalate privileges.
- ▶ Prevention:
  - ▶ • MFA & strong password policy
  - ▶ • Account lockout policy
  - ▶ • Patching & validation



# DoS / DDoS Attack

- ▶ Definition: Flooding systems with traffic to make them unavailable.
- ▶ Types:
  - DoS – single source
  - DDoS – multiple sources (botnet)
- ▶ Examples:
  - SYN flood
  - HTTP flood



# DDoS Scenario & Mitigation

- ▶ Scenario: Gaming website attacked by botnet during new launch.
- ▶ Mitigation:
  - ▶ • Rate limiting
  - ▶ • CDN protection (Cloudflare)
  - ▶ • Traffic filtering & blackholing



## Malicious Code Attack

- ▶ Definition: Malware designed to harm, steal or control systems.
- ▶ Types:
  - ▶ • Virus, Worm, Trojan
  - ▶ • Ransomware
  - ▶ • Spyware, Keylogger
  - ▶ • Botnet agents



## Malicious Code Scenario & Prevention

- ▶ Scenario: Employee opens infected email attachment → ransomware encrypts files.
- ▶ Prevention:
  - Antivirus / EDR
  - Patch OS & apps
  - Backup & awareness training



## Summary & Best Practices

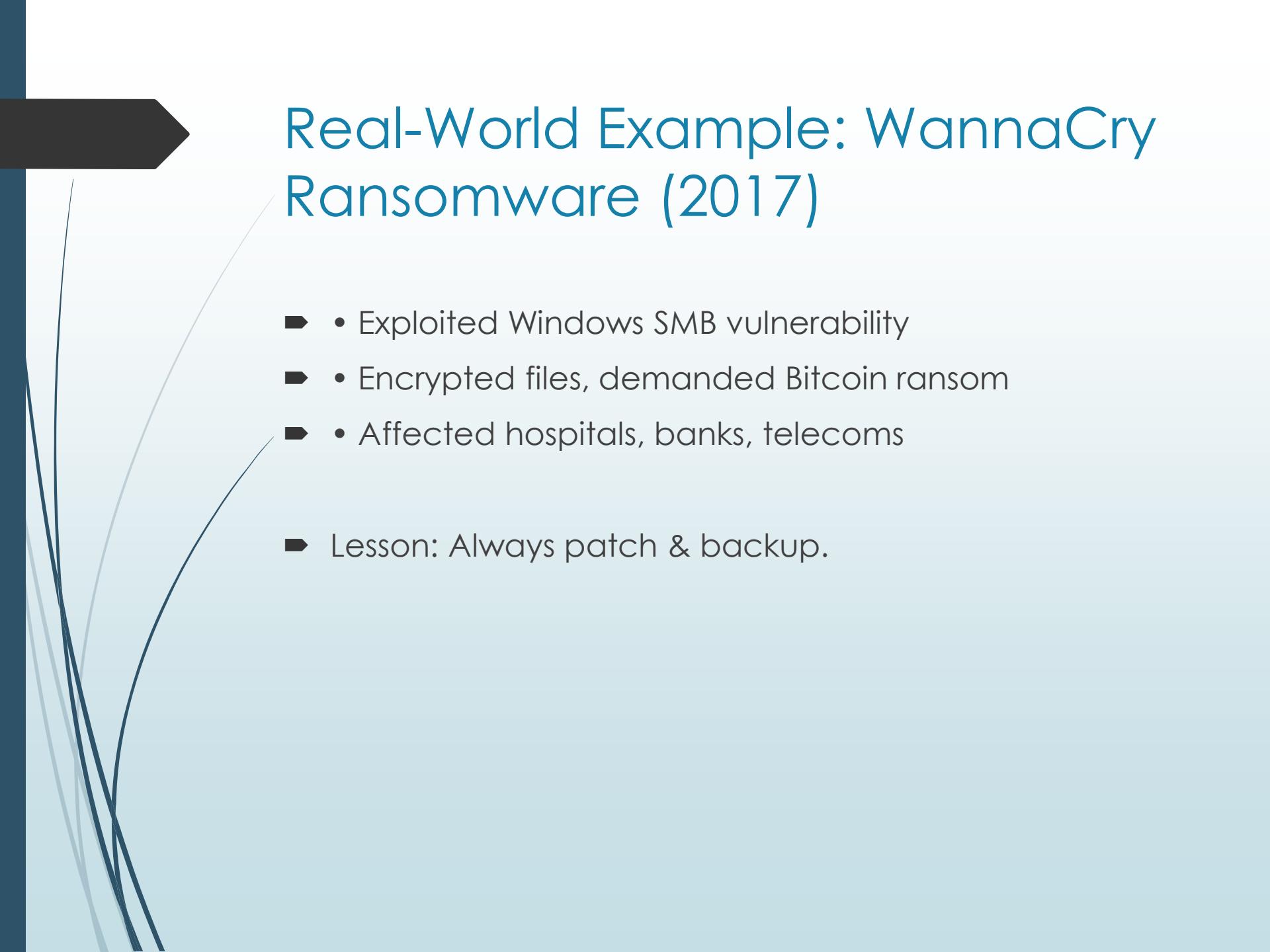
- ▶ • Reconnaissance = Info gathering
- ▶ • Access = Unauthorized entry
- ▶ • DoS/DDoS = Service disruption
- ▶ • Malicious code = Harmful software

- ▶ Best Practices:
- ▶ • Defense-in-depth
- ▶ • MFA
- ▶ • Logging & monitoring
- ▶ • Backups

- 1. List 2 reconnaissance techniques and tools.
- 2. Difference between brute-force & credential stuffing.
- 3. Name 3 ransomware mitigations.

## Group Activity



# Real-World Example: WannaCry Ransomware (2017)

- ▶ • Exploited Windows SMB vulnerability
- ▶ • Encrypted files, demanded Bitcoin ransom
- ▶ • Affected hospitals, banks, telecoms
- ▶ Lesson: Always patch & backup.