# APT

Lecture 6

# What is APT

Advanced Persistent Threats (APTs) are sophisticated and targeted cyberattacks carried out by well-funded and highly skilled threat actors, such as nation-states, organized cybercriminal groups, or advanced hackers. APTs are characterized by their persistence, stealth, and strategic focus on specific targets, typically with the aim of infiltrating and compromising computer systems and networks over an extended period.

# Key Characteristics of APT

1. **Advanced Techniques:** APT actors use advanced and often custom-built malware, tactics, and procedures to carry out their attacks.

2. **Persistence:** APTs aim to maintain unauthorized access to compromised systems for an extended period, remaining undetected.

3. **Targeted:** APT attacks are highly focused on specific organizations, industries, or individuals, often involving extensive reconnaissance.

4. **Stealth:** APTs employ various techniques to evade detection, such as encryption, obfuscation, and anti-analysis measures.

# Key Characteristics of APT (Cont.)

**5. Objectives:** APTs pursue goals like espionage, data theft, intellectual property theft, long-term surveillance, or sabotage.

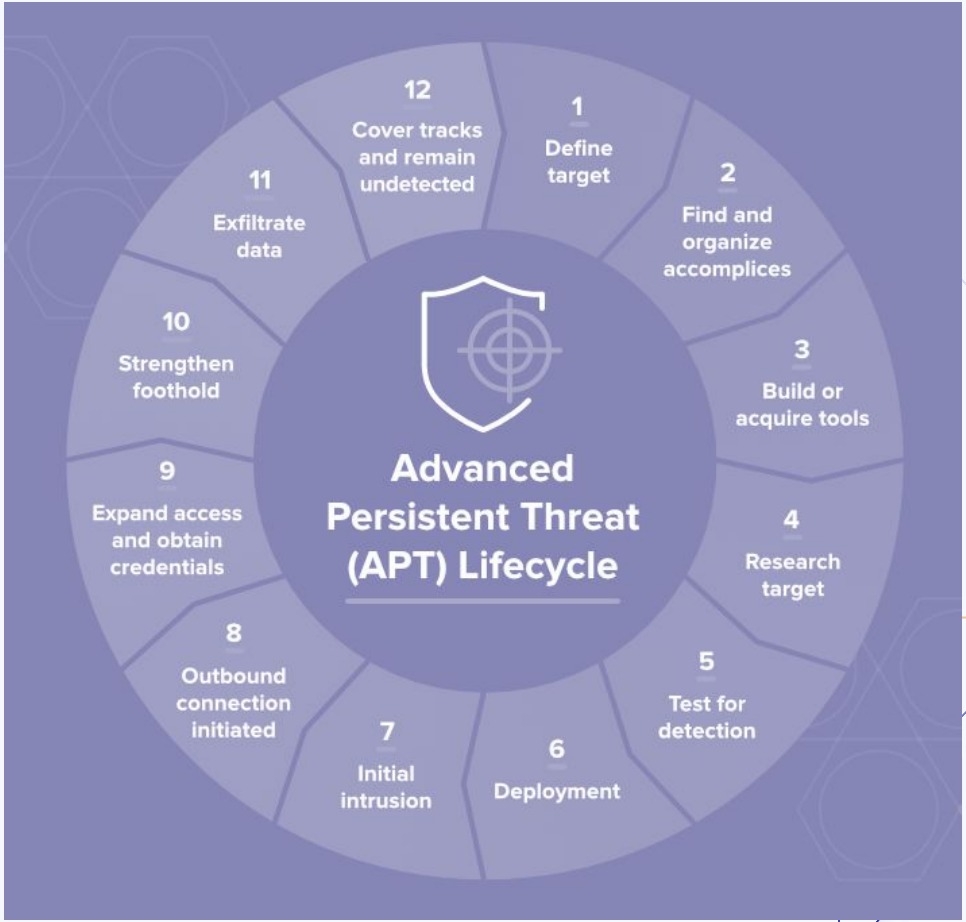
**6. Resourcefulness:** APT actors have significant resources, including financial, technological, and human assets.

**7. Command and Control (C2):** APTs often use remote command and control servers to manage compromised systems and exfiltrate data.

**6. Zero-Days and Exploits:** APTs may employ zero-day vulnerabilities and advanced methods to compromise systems.

# Lifecycle of APT

The Advanced Persistent Threat (APT) lifecycle, often referred to as the APT attack lifecycle, describes the various stages that APT actors typically go through when conducting a targeted cyberattack. It provides insight into how these sophisticated attacks unfold over time. The APT lifecycle stages can vary slightly depending on the source.


Advanced Persistent Threat (APT) Lifecycle
1 Define target
2 Find and organize accomplices
3 Build or acquire tools
4 Research target
5 Test for detection
6 Deployment
7 Initial intrusion
8 Outbound connection initiated
9 Expand access and obtain credentials
10 Strengthen foothold
11 Exfiltrate data
12 Cover tracks and remain undetected

# Lifecycle of APT

**1. Define target:** Determine who you're targeting, what you hope to accomplish – and why.

**2. Find and organize accomplices:** Select team members, identify required skills, and pursue insider access.

**3. Build or acquire tools:** Find currently available tools, or create new applications to get the right tools for the job.

**4. Research target:** Discover who has access you need, what hardware and software the target uses, and how to best engineer the attack.

# Lifecycle of APT

**4. Test for detection:** Deploy a small reconnaissance version of your software, test communications and alarms, identify any weak spots.

**5. Deployment:** The dance begins. Deploy the full suite and begin infiltration.
Initial intrusion: Once you’re inside the network, figure out where to go and find your target.

**6. Outbound connection initiated:** Target acquired, requesting evac. Create a tunnel to begin sending data from the target.

**7. Expand access and obtain credentials:** Create a “ghost network” under your control inside the target network, leveraging your access to gain more movement.

# Lifecycle of APT

**8. Strengthen foothold:** Exploit other vulnerabilities to establish more zombies or extend your access to other valuable locations.

**9. Exfiltrate data:** Once you find what you were looking for, get it back to base.

**10. Cover tracks and remain undetected:** The entire operation hinges upon your ability to stay hidden on the network. Keep rolling high on your stealth checks and make sure to clean up after yourself.

# Questions

# Thanks!