- Filename: eccouncil-ceh31250-v11-7-2-1-apt.md
- Show Name: CEHv11 (312-50)
- Topic Name: System Hacking Phases and Attack Techniques - Malware Threats
- Episode Name: APT
  ==========

# APT

# Objectives:

- Define APT
- List and explain the common attributes of APT
- Define and describe the phases of the APT lifecycle

---

- Today we're discussing APT, and I've heard this term thrown around in the Cyber Security space quite a bit, but there seems to be some mystery surrounding the idea. Can you help clear this up a bit for us and define APT?
    - Advanced Persistent Threat
        - Can be used in reference to APT GROUPS and their capabilities, sophistication, and objectives
            - Fancy Bear (Russia, APT 28)
            - Lazaraus Group (N.Korea, APT 38)
            - https://attack.mitre.org/groups/
            - https://www.fireeye.com/current-threats/apt-groups.html
            - https://securelist.com/apt-trends-report-q1-2021/101967/
        - Also used to reference the malware used by these groups
- Let's dig into the details of those APT characteristics.
    - Goal Oriented
        - They are after sensitive information
            - That info could be...
                - PHI
                - PII
                - State Secrets
                - Intellectual Property
                - Financials
                - Research and Development
                - Political or Activists Statements
        - Long-Term Access
            - No smash and grab!
            - They look to maintain access for as long as possible
        - Patient
            - Which in turn makes them stealthy
        - Highly Skilled
            - Develop custom Zero-day exploits
            - Advanced competency in multiple OSs, networking, programming, web, etc
            - Able to evade security controls
            - Attack from multiple vectors
            - Multi-staged attacks

        - Resourceful
            - Living off the Land
            - Command and Control access

- Now that we know what APT is and their attributes, let's turn our attention to the APT Lifecycle. What is the APT Lifecycle and what are its details we need to be aware of?
    - 'step-by-step' of phases that APT typically goes through when attacking a target
        - 6 phases
            - Preparation
                - Choosing and defining a target
                - Intelligence gathering
                - Acquire or create tools
                - Test for detection
            - Initial Intrusion
                - Malware deployment
                - Establish a connection
            - Expansion
                - Expand Access
                - Gather Creds
            - Persistence
                - Maintaining Access
            - Search and Exfil
                - Gather sensitive data
                - Exfil data to attacker controlled device
            - Cleanup
                - Covering Tracks
                - Persist undetected for as long as possible