Advanced Persistent Threat (APT)

U.S. ARMY

(U) This infographic provides an overview of Advanced Persistent Threat (APT), a type of cyber attack in which an unauthorized actor gains access to a computer network and remains there for an extended period, often with the intention of stealing sensitive information or disrupting the network's operations.

Characteristics of APTs:

- Advanced: APTs use sophisticated techniques and tools to evade detection and breach security defenses.
- Persistent: APTs remain in the network for an extended period, often months or even years, to gather intelligence, steal data, and/or disrupt operations.
- Threat: APTs are designed to cause harm by stealing sensitive information, disrupting operations, or setting conditions for future attacks.

Goals of APTs:

- Espionage: Stealing sensitive information, such as intellectual property, trade secrets, or national security information.
- Sabotage: Disrupting operations, such as shutting down critical infrastructure or disrupting supply chains.
- Financial gain: Stealing financial information, such as credit card numbers or personal identifiable information (PII).

Tactics, Techniques, and Procedures (TTPs) of APTs:

- Spear phishing: Targeted phishing attacks to gain initial access to the network.
- Malware: Using custom-built malware to evade detection and maintain persistence.
- Lateral movement: Moving laterally within the network to gain access to sensitive areas.
- Command and control (C2): Establishing a C2 channel to communicate with the attacker's infrastructure.
- Data exfiltration: Stealing sensitive information and exfiltrating it from the network.

A few known APT groups

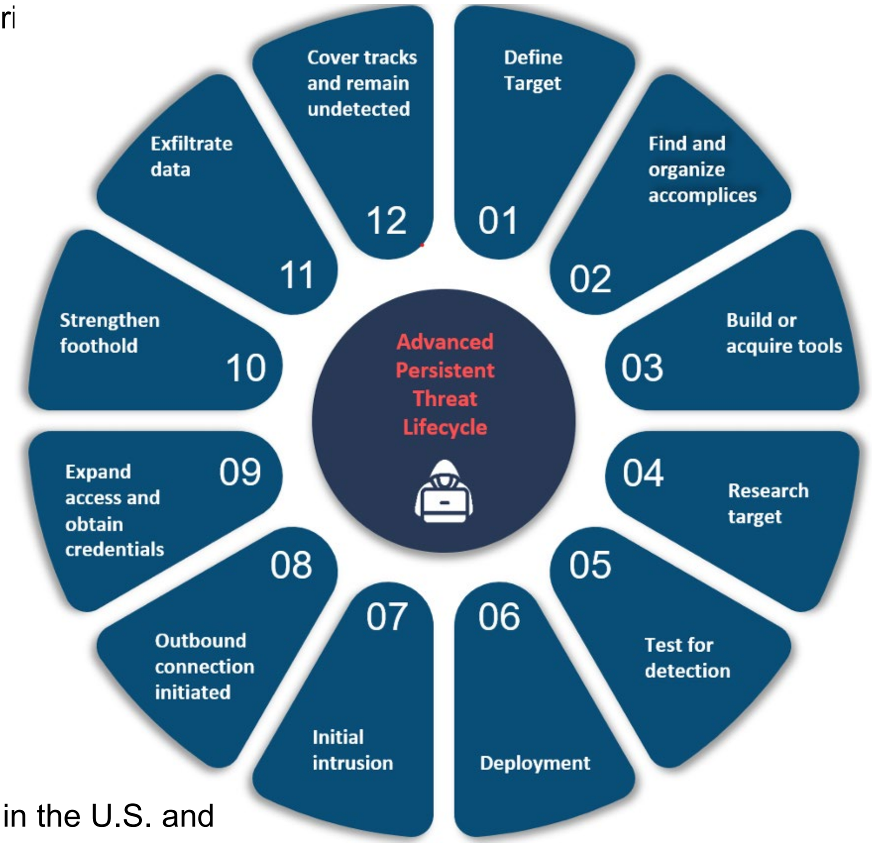
APT1 (Comment Crew): A Chinese APT group known for targeting U.S. defense contractors and stealing sensitive information.

APT10 (Stone Panda): A Chinese APT group known for targeting technology and aerospace companies in the U.S. and other countri

APT28 (Fancy Bear): A Russian APT group known for targeting government agencies, defense contractors, and other organizations in the U.S. and Europe.

APT32 (Ocean Lotus): A Vietnamese APT group known for targeting companies in the aerospace and defense industries.

APT33 (Elfin): An Iranian APT group known for targeting companies in the aerospace and defense industries.



Advanced Persistent Threat Lifecycle

01 Define Target

02 Find and organize accomplices

03 Build or acquire tools

04 Research target

05 Test for detection

06 Deployment

07 Initial intrusion

08 Outbound connection initiated

09 Expand access and obtain credentials

10 Strengthen foothold

11 Exfiltrate data

12 Cover tracks and remain undetected

Notable APT Activity

Operation Aurora: A series of attacks targeting major corporations, including Google, Adobe, and Microsoft.

Sony Pictures hack: A devastating attack resulting in the theft of sensitive information, including employee data and unreleased movies.

Election hacking: A series of attacks targeting election systems in the U.S. and other countries.

NotPetya: A highly destructive ransomware attack targeting companies in Ukraine and other countries..

The attribution of APT groups to specific countries is not always clear-cut, and some groups may be sponsored by multiple countries.

Source: APT Buyers Guide (GSA); Advanced Persistent Threat (APT) (CowdStrike); Nation-State Cyber Actors (CISA)