# Discussing Advanced Persistent Threats (APT)

**Dale Meredith**
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith|

Success is a lousy teacher. It seduces smart people into thinking they can’t lose

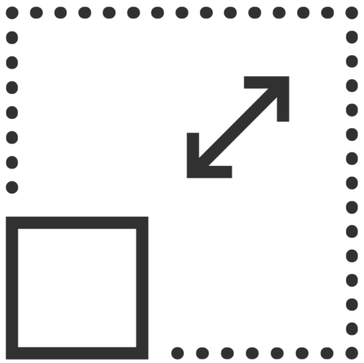
**Bill Gates**

## What is an Advanced Persistent Threat

A network attack that remains undetected for a long time

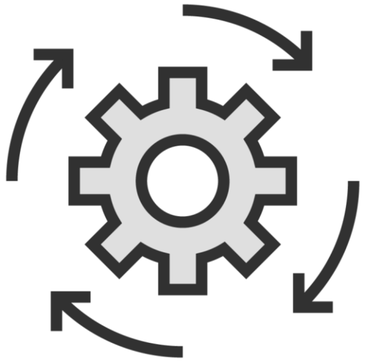
# Advanced Persistent Threat

**Involves well-planned and coordinated techniques that erase evidence of the attackers malicious activities after their objectives have been fulfilled.**



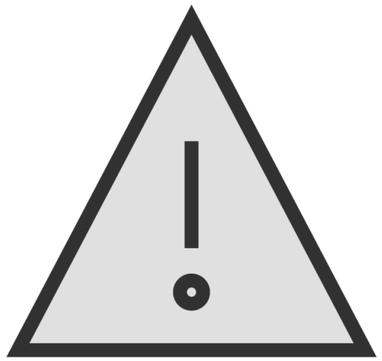
## Advanced

Signifies the use of techniques that exploit



## Persistent

References the external command-and-control (C&C)



## Threat

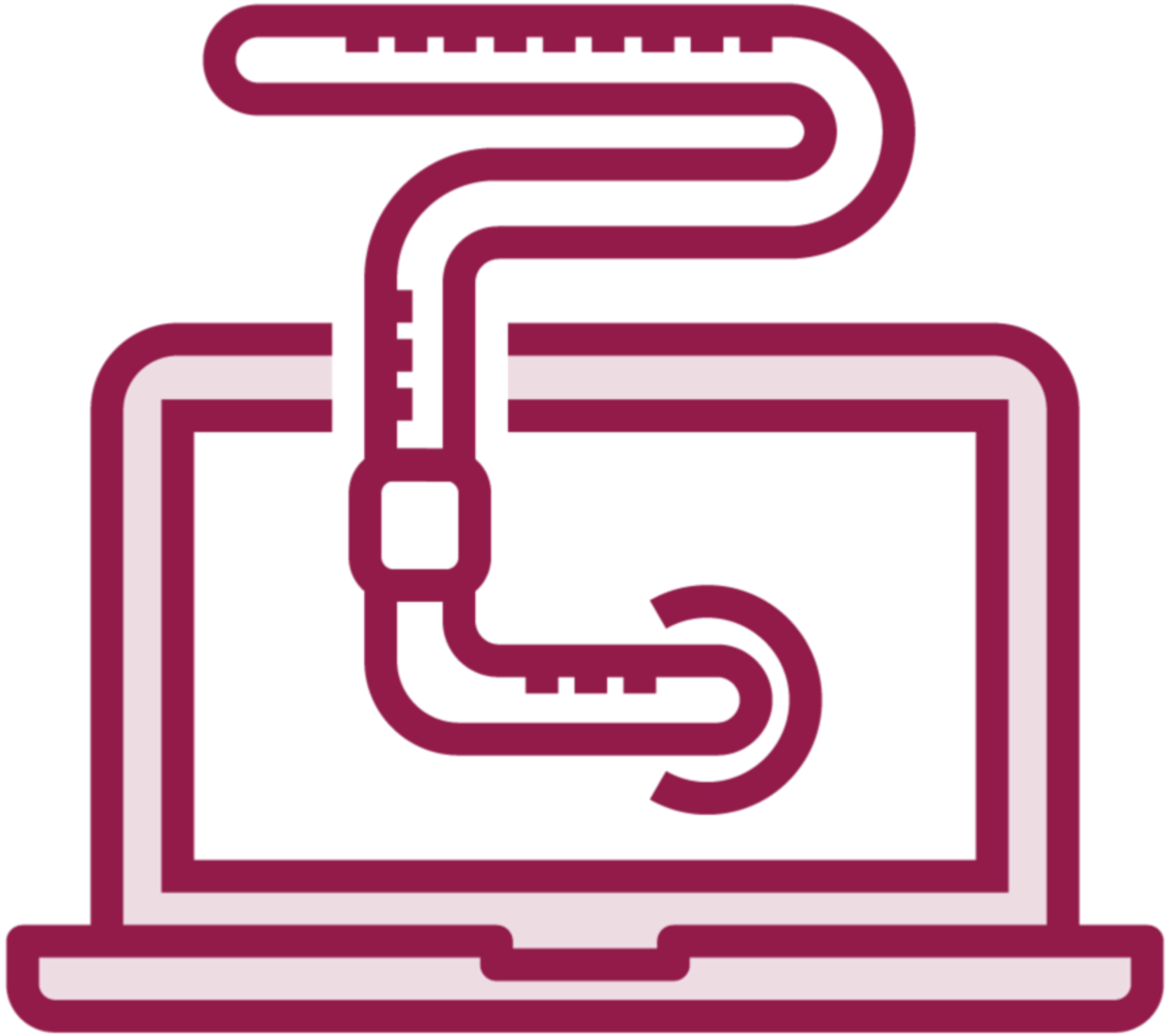
Signifies human involvement and coordination

# Information Obtained

| | | | |
|---|---|---|---|
| **Classified documents** | **User credentials** | **Personal information** | **Network information** |
| **Transaction information** | **Credit card information** | **Business strategy** | **Control system access** |

The main objective is to obtain sensitive information rather than sabotaging a network.

# Stuxnet Worm



# APT Characteristics

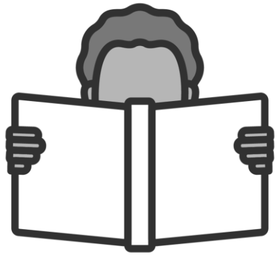
# Characteristics are the what, how, and why attackers design and plan their attacks

**Objectives**

**Timeliness**

**Resources**


**Risk Tolerance**

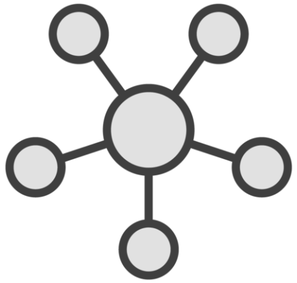


**Skills and Methods**

**Actions**

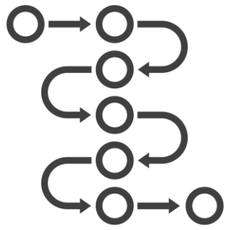
# Characteristics are the what, how, and why attackers design and plan their attacks

**Attack Points**

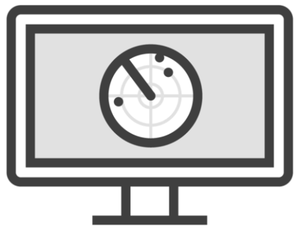


**Numbers Involved**

**Knowledge Source**



**Multi-phased**

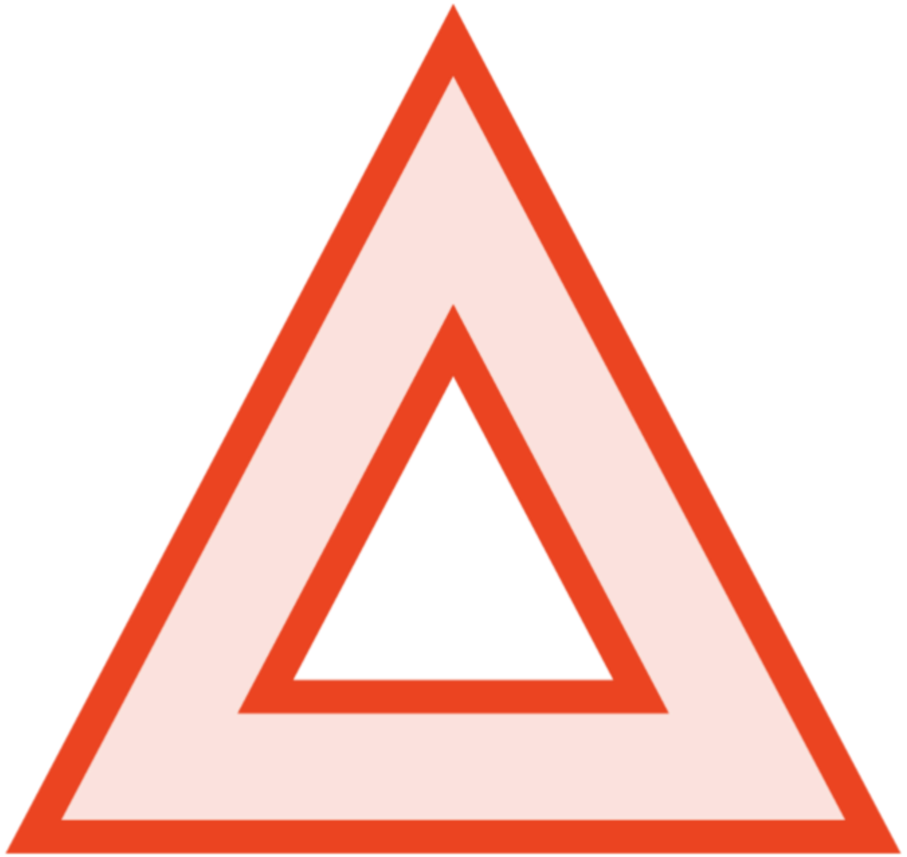


**Tailored to Vulnerabilities**

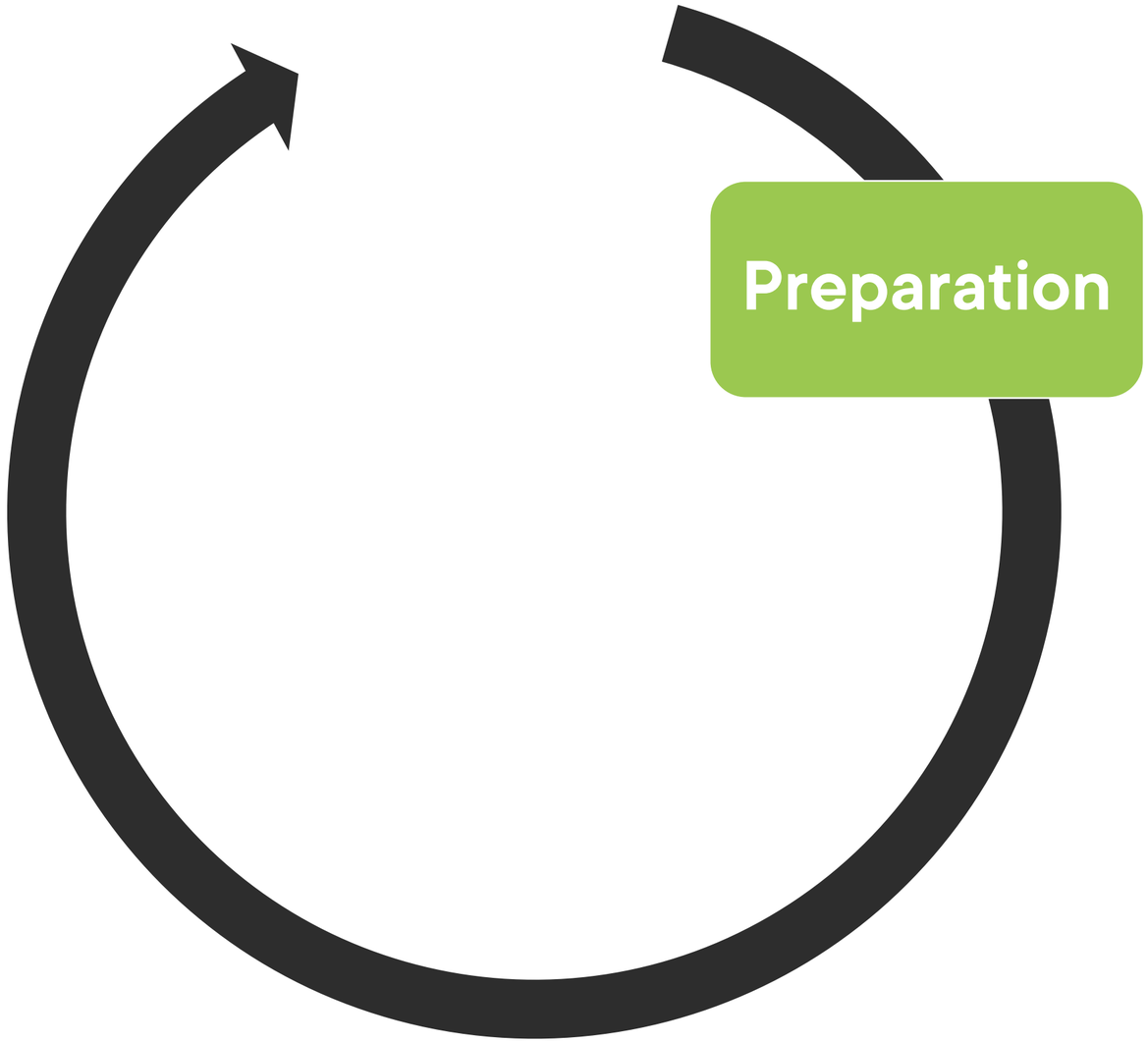
**Multiple Entry Points**

# APT attacks easily bypass security mechanisms

# Warning signs



# Lifecycle of a APT



# Preparation

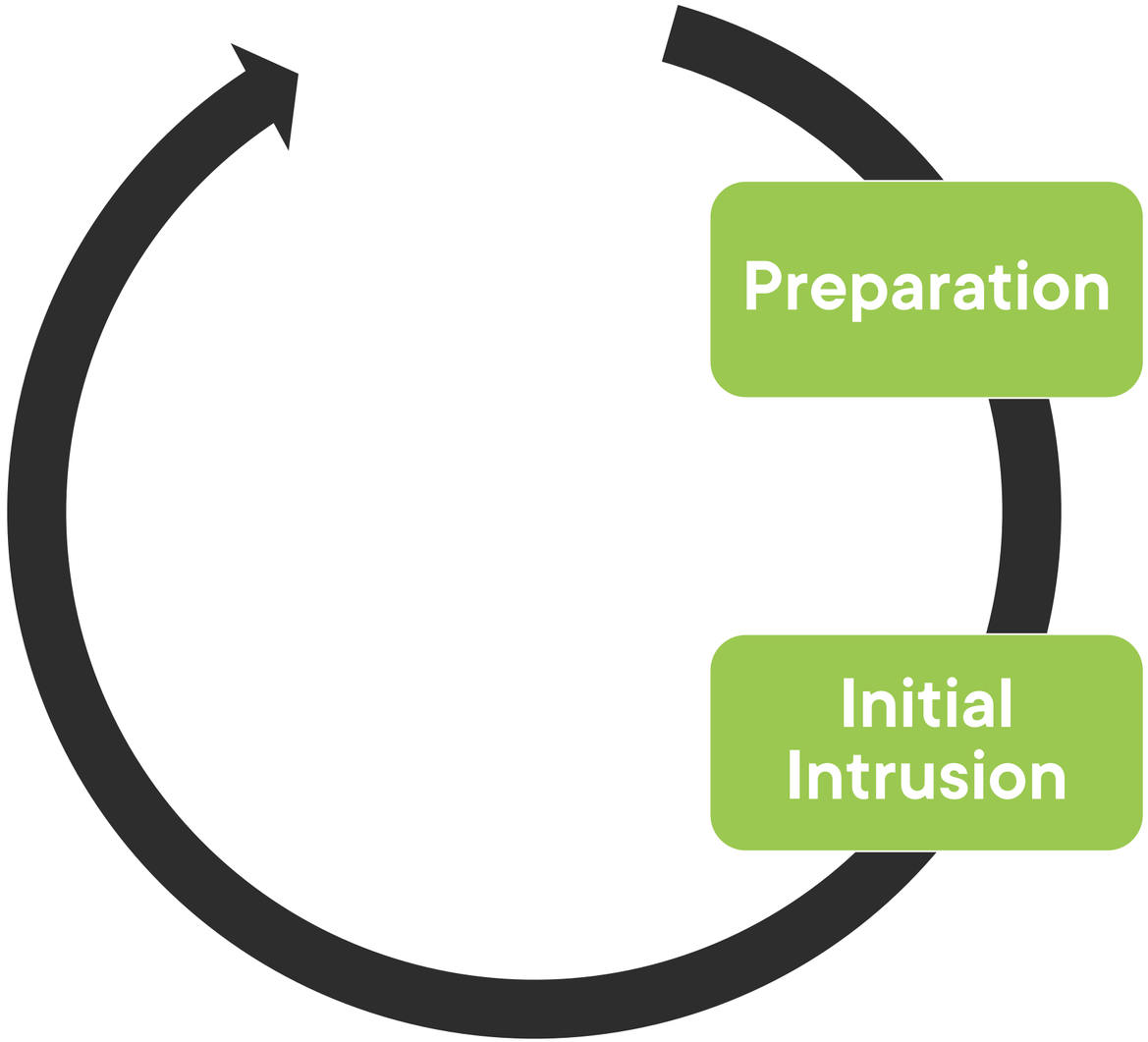
**Defines**

**Researches**

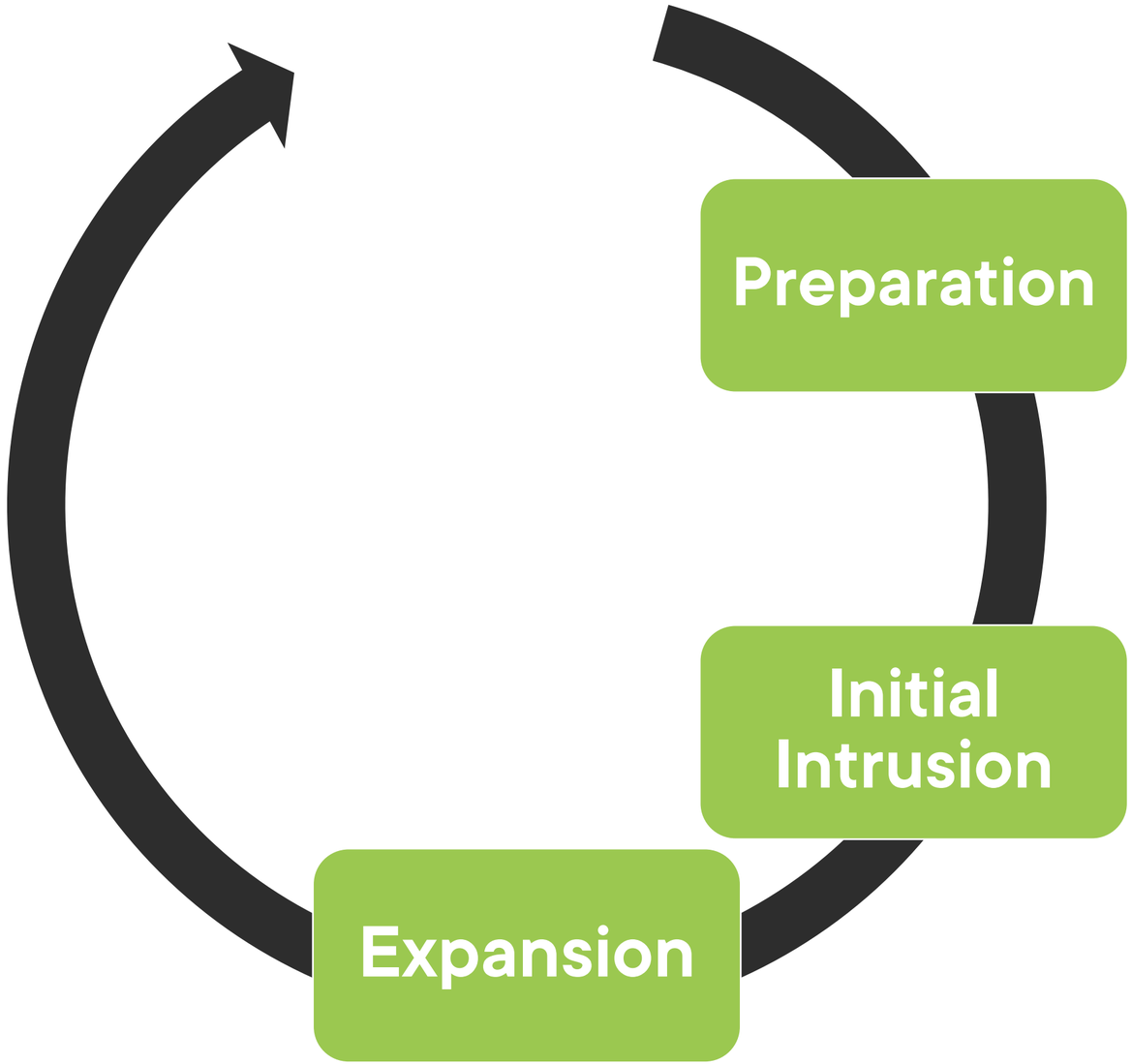
**Organizes a team**

**Builds or attains tools**

**Performs test**

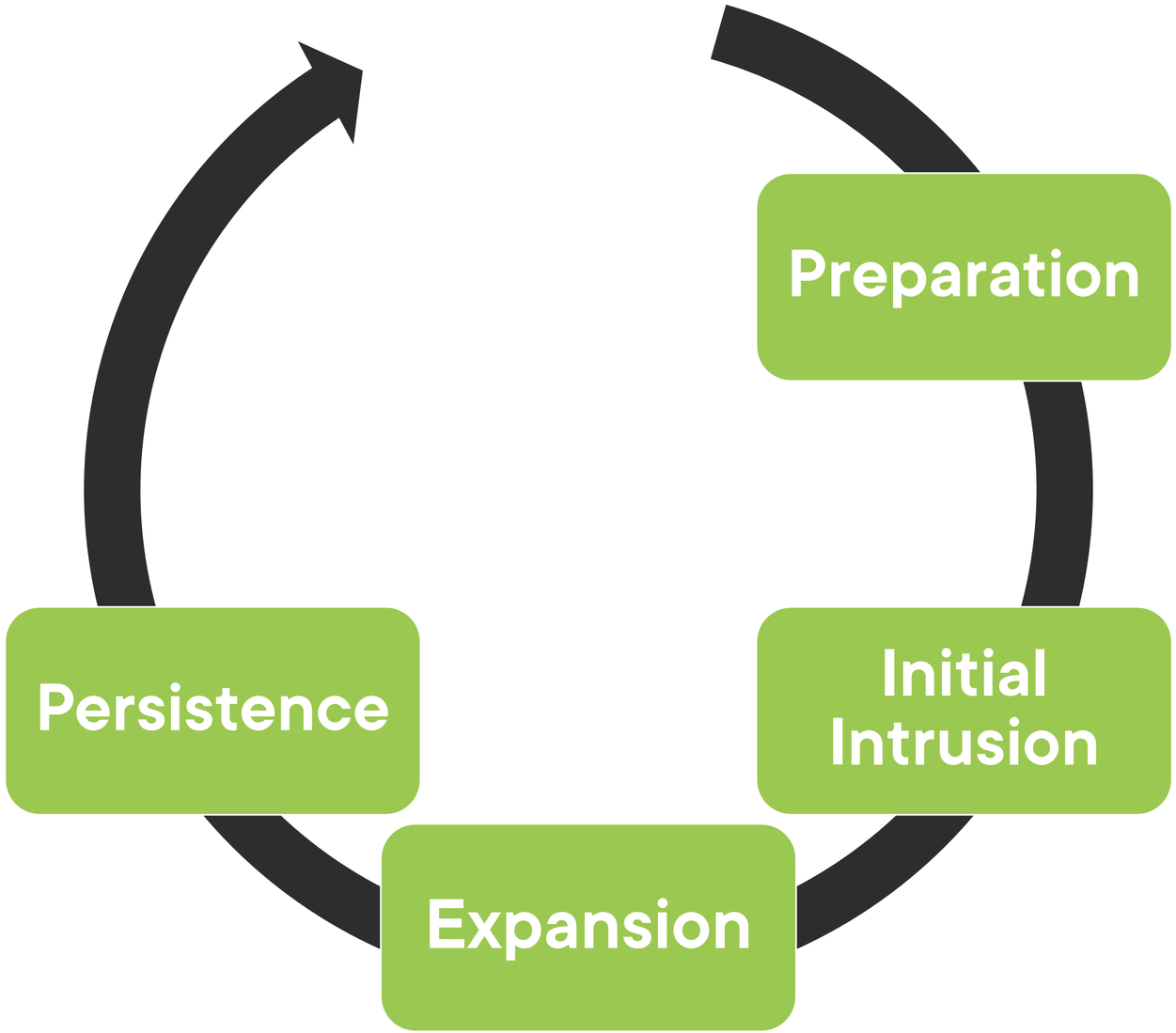


# Initial Intrusion



# Expansion

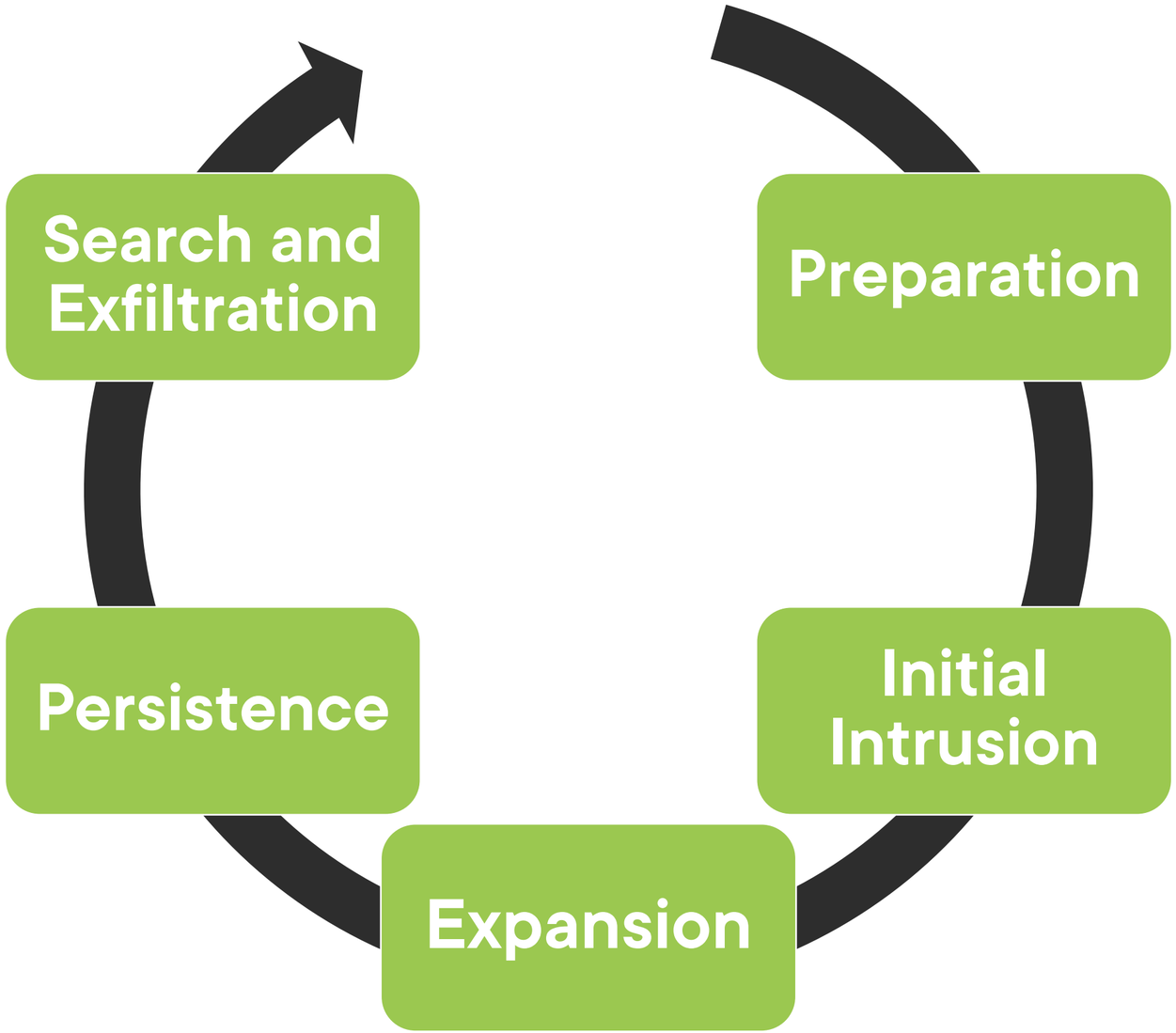
**Attacker will need to obtain administrative credentials to escalate privilege and to gain further access**



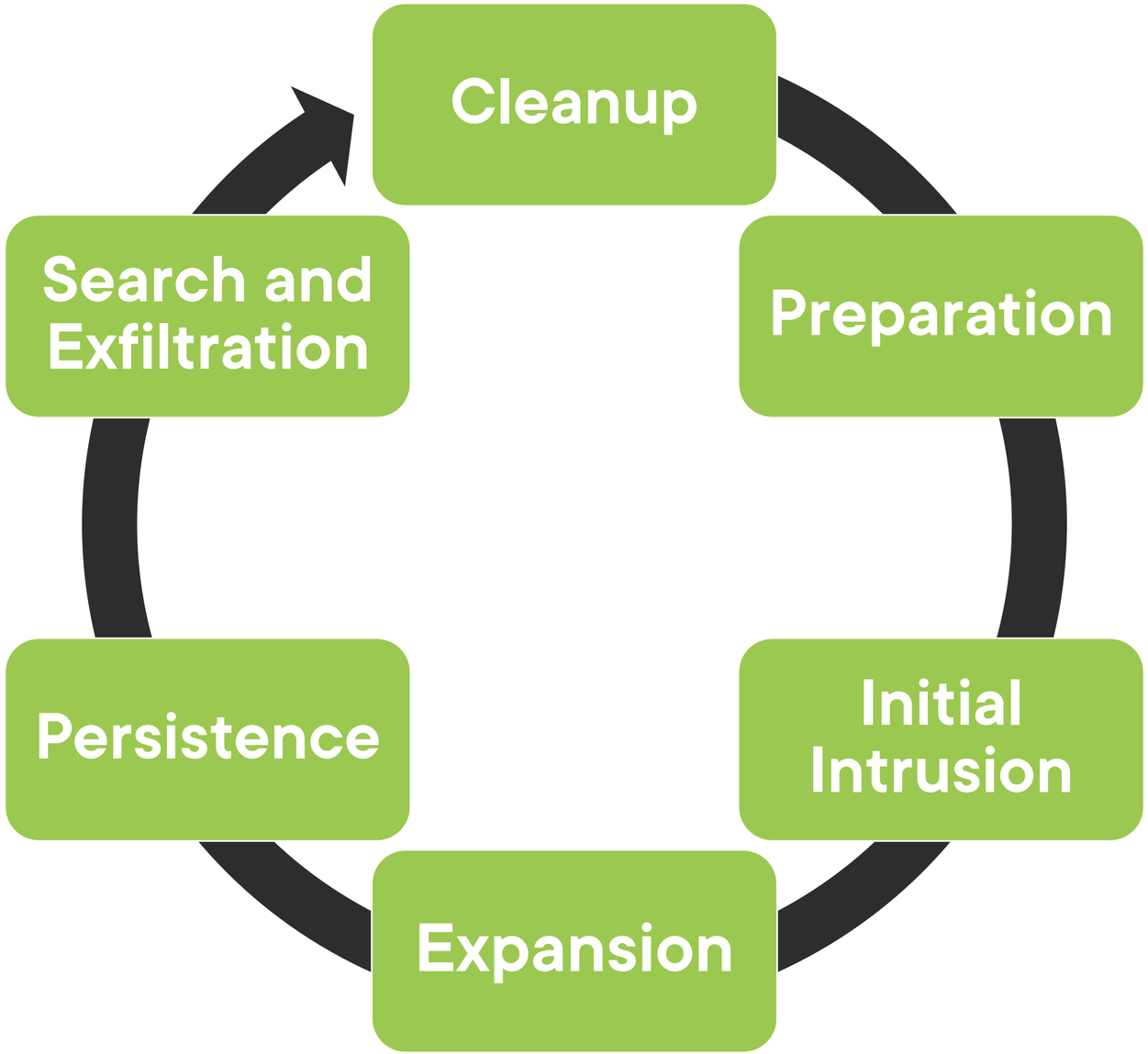
# Persistence

**Use customize malware that includes services, executables and drivers installed on the targets network**

**Find locations for installing malware that are not frequently examined**

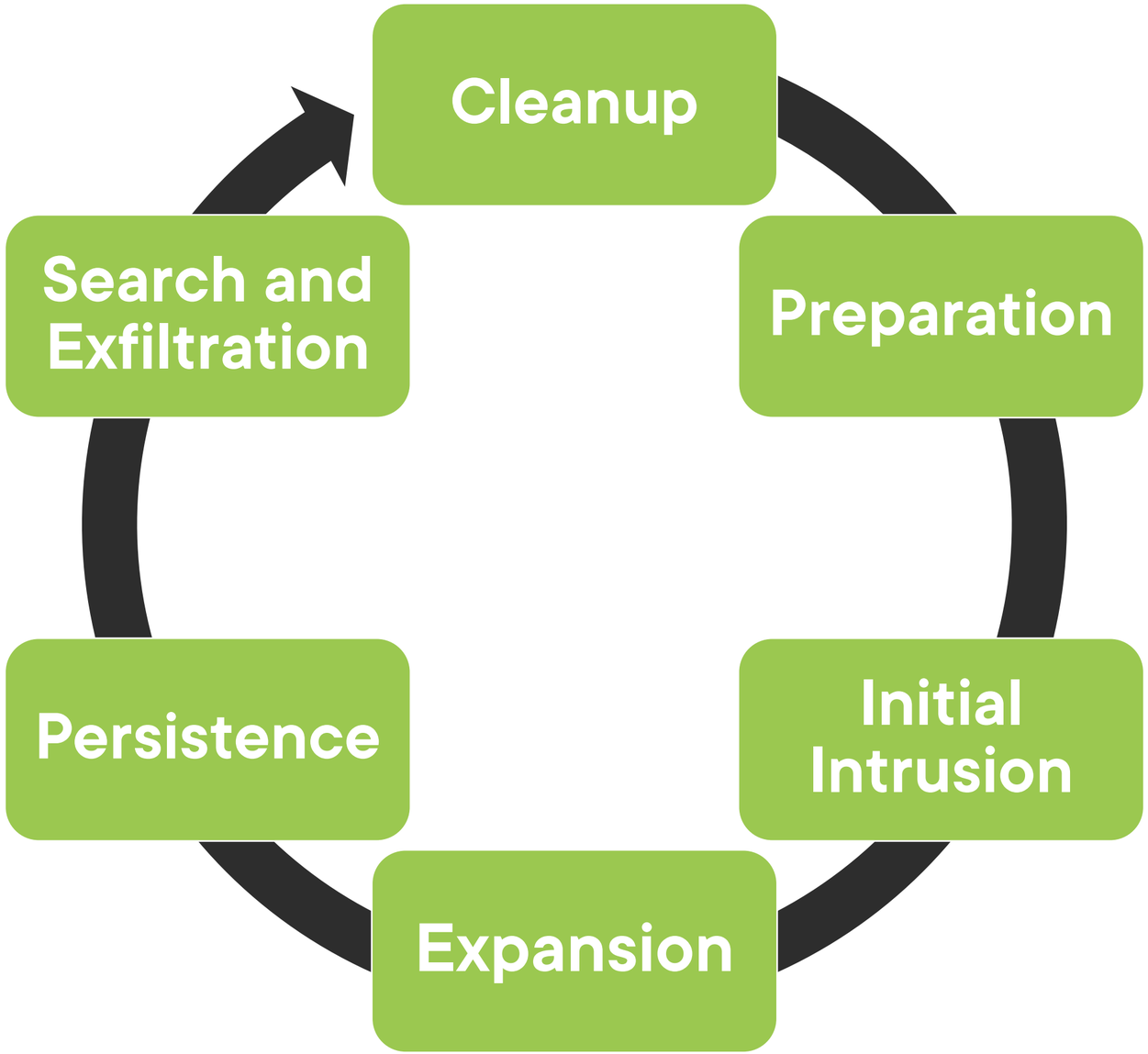


# Search and Exfiltration



# Cleanup

**Prevent detection by covering their tracks**



# Learning Check

# Learning Check

- Obtain data rather than destructive tasks
- Cleanup
- Initial intrusion
- Expansion
- Nation state actors

# Up Next:
# Explaining Trojans