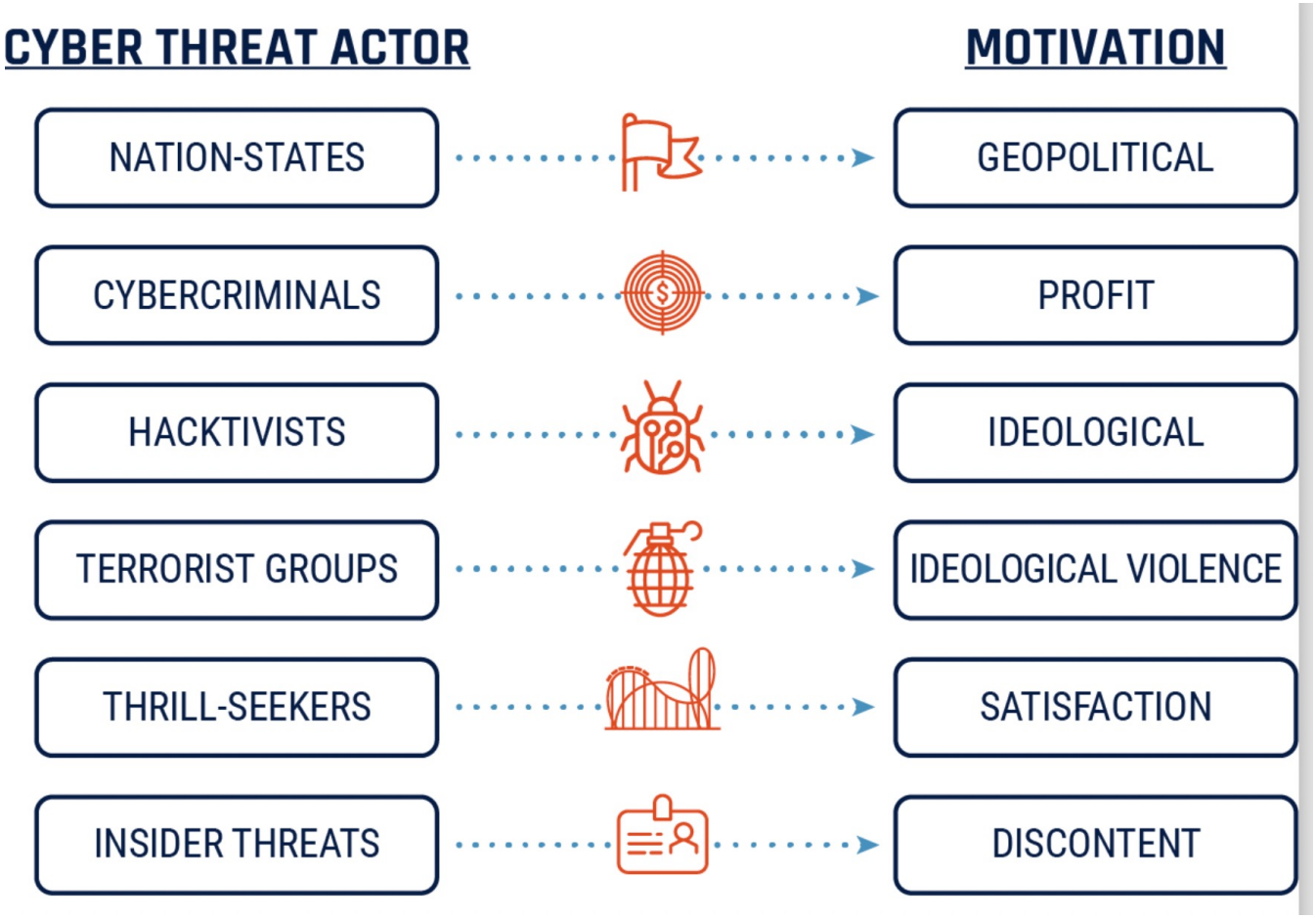
Agenda

Cybercrime Actors

At the end of this week, students should be able to:

1. Understand the role played by the various cybercrime actors namely the cybercriminals, cyber-victims and cyber-investigators
2. Define the terms hacker, cracker, script-kiddie, blackhat, greyhat and whitehat
3. Discuss the profile of a cybercriminal and contrast this to existing stereotypes
4. Describe the role of cybercrime and forensic investigators and the work that they do from when a crime is committed till a cybercriminal is apprehended

Cyber threat actors



Sample Cyber criminal Threat Actors

Threat Actor	Description and Motivation	Potential Targets	Goal
Cyber Criminal	Varying degree of competence. Usually motivated by the achievement of financial gain or the affirmation of private justice	Potentially any target for personal reasons or as “for-hire guns” by a third party threat actor	Financial gain, private justice
Organized Crime	Structured, funded, consisting of different roles with associated competences and responsibilities. Usually motivated by the achievement of financial gain. Can be hired by other threat actors (e.g. industrial espionage, internal threats etc.)	Commercial organization but potentially any target as “for-hire guns” by a third party threat actor	Financial gain
Hactivists	Typically decentralized groups or individuals with varying degree of technical skills. Highly motivated by their ethics and principles and the advancement of a cause	Targets are specific to the sectors of interest to the activist group (environmentalist, animal lovers etc.)	To cause reputational damage or advance specific causes through information gathering
State-sponsored criminals	Technically skilled with virtually unlimited resources at their disposal, motivated by the country political agenda	Foreign government institutions and officials, large foreign commercial organizations	Acquire information, monitor and control
Competitors/ Industrial Espionage	Good level of resources and varying degree of comptences, usually motivated by the achievement of business objectives	Targets varies according to the relevance to the threat actor	Acquire information, disrupt business (image, reputation and operations)
Employees/Internal Threat	Quite varied in age, techinal competence and intent but all in possession of sensitive information that has a critical impact to the organization. Can be used by other threat actors. Motivated by malcontent, spirit of revenge or financial gain	Typically commercial organizations but potentailly applicable to any type of organization	Personal gain or revenge
Opportunists	Unaffiliated hackers (usually young) looking for recognition by the hackers community and for new learning opportunities. Rarely financially motivated	Various targets both from the private and public sectors. Target sensitivy varies with the capability of the threat actor	Achieve recognition, improve competence

The role played by the various cybercrime actors

- Threat Actors
  - Different types, motivations, targets
- Goals and Strategy
  - Define what the attackers want and how the plan to achieve it
- Tactics Techniques and Procedures
  - Define what the attackers will do to implement their strategy and achieve their goals
- Indicators
  - Define the evidence left behind by the attackers

Types of Threat Actors

- There are several types of malicious actors. Most fall under the standard cybercriminal insider threat actors
- **Insider Threats**
- Investigations Report,
- Insider Threat Indicators.
- **Nation-state Threat Actors**
- **Motivations for Threat Actors**
- **How to Stay Ahead of Threat Actors**

The Kill Chain

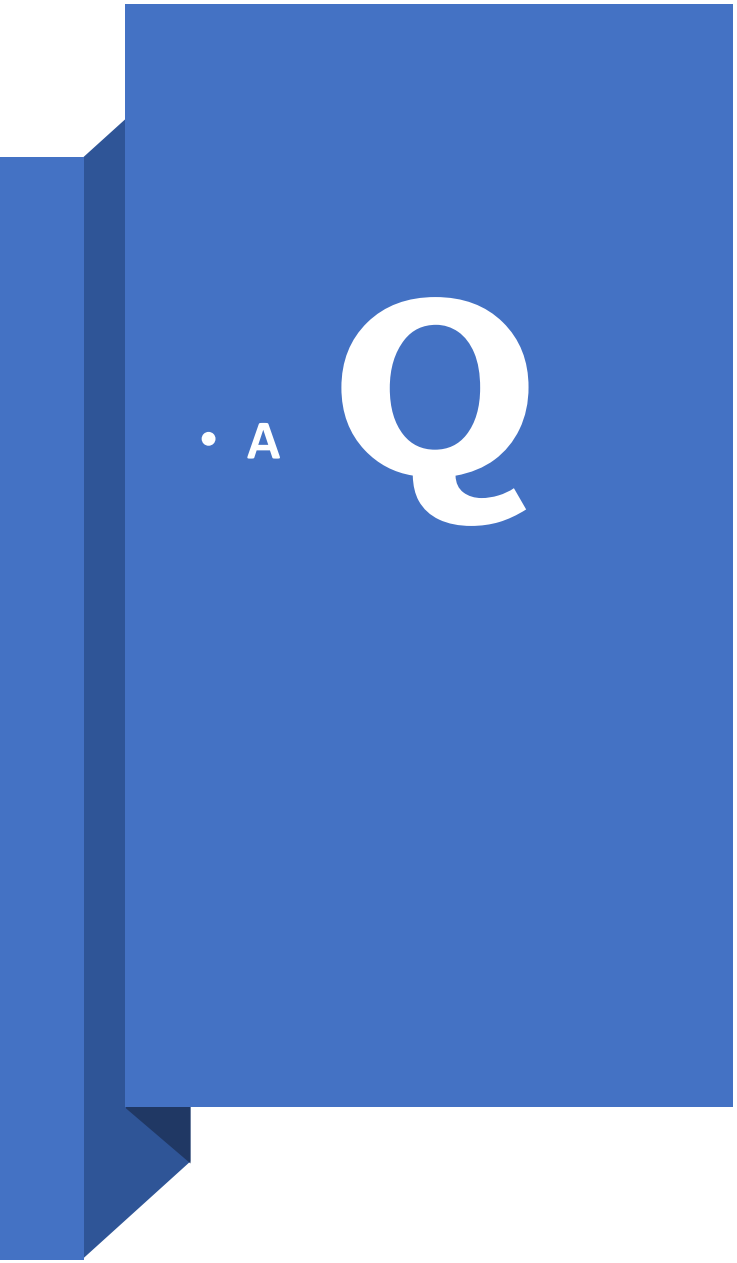
- Systematic process of finding and engaging an adversary to create the desired effects (US Army, 2007)
  - Adapted by Hutchins et al. in 2011
- Key observations
  - Going from the Recon phase to the final Action phase is NOT immediate
  - The time taken for the kill chain process to execute can be used to gather intelligence and capabilities to interfere with each step of the kill chain.

Phases of the Intrusion Kill Chain

Reconnaissance	Research, identification, and selection of targets
Weaponization	Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files)
Delivery	Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)
Exploitation	Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems
Installation	The weapon installs a backdoor on a target's system allowing persistent access
Command & Control	Outside server communicates with the weapons providing "hands on keyboard access" inside the target's network.
Actions on Objective	The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target

What is Threat Intelligence

- *“Details of the motivations, intent, and capabilities of internal and external threat actors. Threat intelligence includes specifics on the tactics, techniques, and procedures of these adversaries. Threat intelligence's primary purpose is to inform business decisions regarding the risks and implications associated with threats”* (Forrester)


A
Q


Q
&
&
A