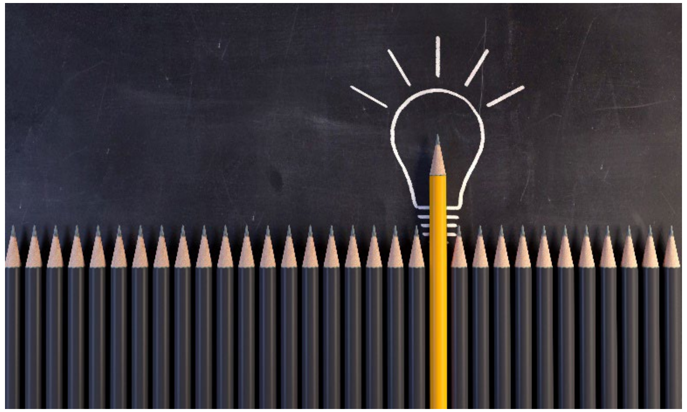
02-Threat Actors, Attack Vectors, and Impacts

Learning Objectives

- Discriminate between threat actors based on their attributes.
- Identify common attack vectors.
- Explain how the security of a system's components might impact the security of the system.
- Describe types of social engineering attacks.



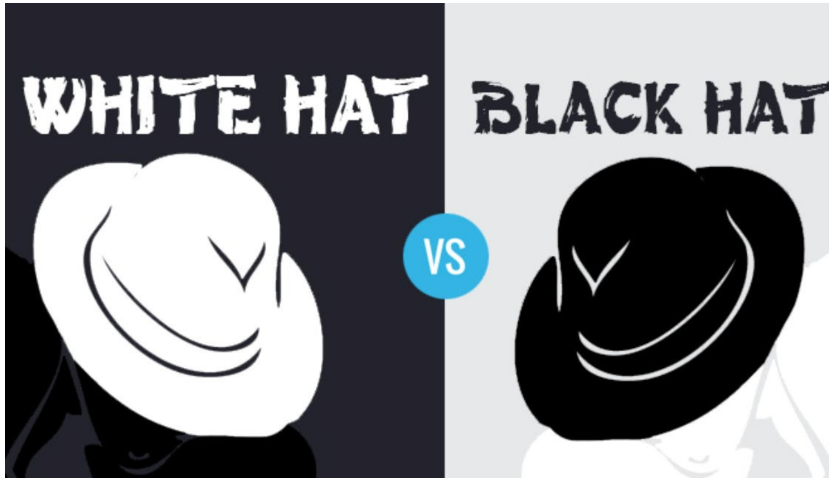
Threat Actors

- A threat actor (attacker) is an individual or entity responsible for cyber incidents against the technology equipment of enterprises and users.
- Cybercrime is often divided into three categories based on targets:
  - Individual users:
    - Stealing personal data (e.g., credit card numbers) to make profit.
  - Enterprises:
    - Stealing research/design documents of a product and selling them to competitors.
  - Governments:
    - Spying on governments to steal defense plans or publishing secret information to embarrass them.

Types of Attackers

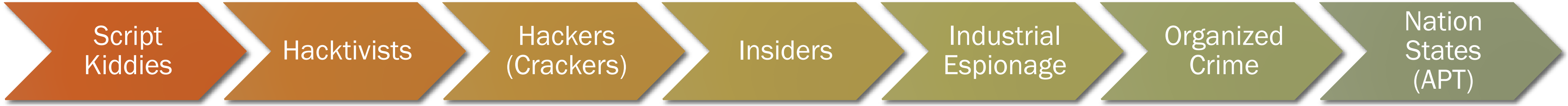
The term hacker is used to refer to a person with high computer skills. Hackers can be classified into:

- Black hat hackers: violate computer security and may cause damage for personal gain.
- White hat hackers: take permission to probe an organization's system for weaknesses and report the findings.
- Gray hat hackers: attackers who attempt to break into a system without permission (an illegal activity) and disclose the results to cause embarrassment and push for action, not for their own advantage.



Types of Attackers

Today, threat actors are classified in more distinct categories:



Script Kiddies

Hacktivists

Hackers (Crackers)

Insiders

Industrial Espionage

Organized Crime

Nation States (APT)

- Script kiddies: individuals who want to perform attacks yet lack technical knowledge and use freely available attack tools to carry them out.
- Hacktivists: are strongly motivated by ideology (for the sake of their principles or beliefs). They often want to make a political statement or push for a change.
- Insiders: often a trusted employee, contractor, or business partner who may cause damage.
- Industrial espionage: competitors launching attacks against their opponents.
- Criminal syndicates: groups of hackers, developers, and other tech outlaws who collaborate to perform massive crimes such as heists, blackmail, cyber terrorism, etc.

Types of Attackers

- State actors: are sponsored by states/governments for launching cyberattacks against their enemies. These are usually:
  - equipped with state-of-the-art technology,
  - involved in multiyear intrusion campaigns targeting highly sensitive economic, proprietary, or national security information,
  - and associated with the deadliest attack (called advanced persistent threat APT).

(Video 3:08, The Secret Lives of Hackers)

Question

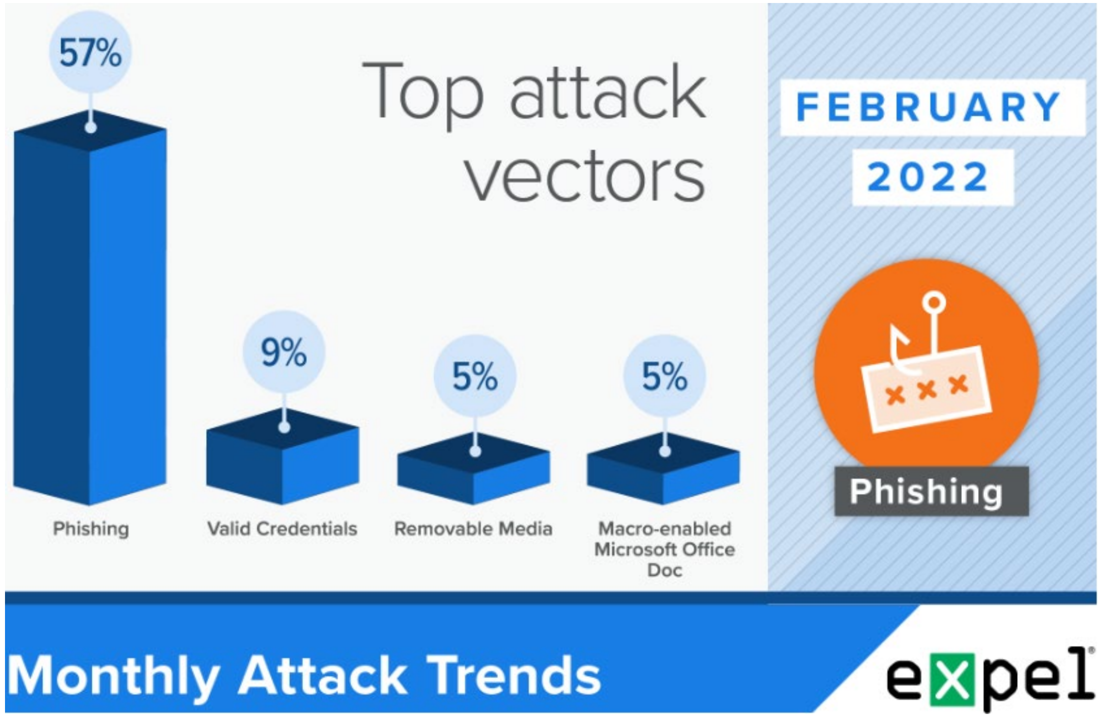
- A group of threat actors launched an attack against a system belonging to a bank that froze some accounts belonging to their supporters. Which category could these attackers be classified into?
    - Script Kiddies.
    - Industrial espionage groups.
    - Criminal syndicate group.
    - State actors.
    - Hacktivists.

Attack Vectors

An attack vector is a pathway used by a threat actor to penetrate a system.

Attack vectors can be classified into:

- Email: trick the recipient to click a malicious link or open an attachment.
- Wireless: data carried through airwaves can be easily intercepted in unsecured wireless networks.
- Removable media: USB drives can be infected with malware and intentionally given/left to users who pick them up.
- Direct access: physical access to computers or network devices poses the most dangerous threat. Direct access to a device makes it a lot easier to hack it than remote access.



Attack Vectors

- Social media: information posted on social media may help the attacker determine the right time and method of attack (e.g., when an employee is on vacation).

  (Video 3:27, A Cyber Privacy Parable)

- Supply chain: a supply chain is a network that moves a product from the supplier to the customer and is made up of vendors, manufacturers, warehouses, distribution centers, and retailers. With so many businesses involved, an attack could be carried out on a part of the network (the weakest link) which propagates to other parts.

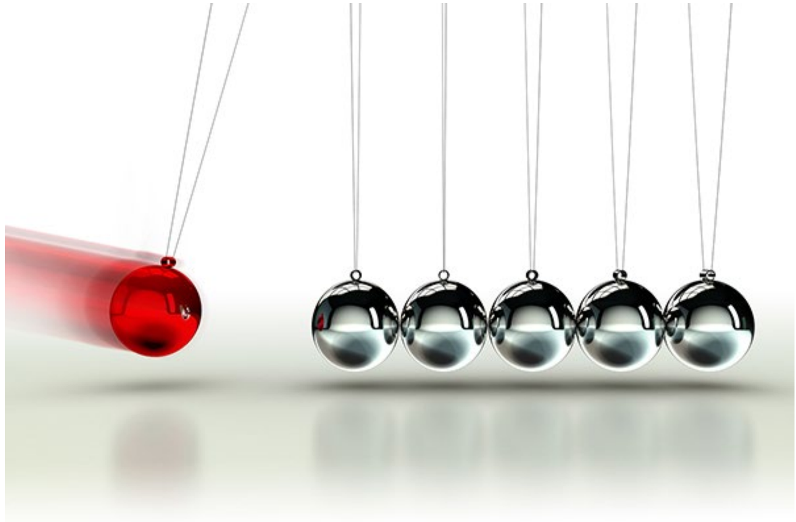
  (Video 2:58, What is a Supply Chain Attack?)

- Cloud: as enterprises move their computing resources to remote cloud servers and storage devices, threat actors take advantage of the complexity of these systems to find security weaknesses.

Impacts of Attacks

A successful attack always results in several negative impacts.

- Data impacts: while the goal of some attacks may be harm to a system, data is becoming the primary target. Impacts on data could take one of the forms:
  - Data loss: destroying data beyond recovery, e.g., erasing students' records from a university system.
  - Data exfiltration: stealing data to distribute it to other parties, e.g., stealing the list of customers and selling it to a competitor.
  - Data breach: stealing data to disclose without authorization, e.g., stealing account information of a social media platform and dumping it on the public internet.
  - Identity theft: taking personally identifiable information (PII) to impersonate someone, e.g., getting social security number of someone to apply for credit card under their name.



Impacts of Attacks

- Effects on the enterprise: enterprises could be impacted in several ways due to a successful attack:
  - Availability: an attack could make the system of an enterprise unavailable.
  - Reputation: customers could lose trust or change their perception of the enterprise.
  - Financial loss: an enterprise may have to pay for the repairs and may suffer from drop in sales & revenue due to customer loss.

Social Engineering Attack

- Social engineering is a means of gathering data by relying on the weaknesses of individuals.

  (Video 2:49, What is Your Password?)

- Attackers often rely on psychology to affect others mentally and emotionally, some examples are:
  - Exhibiting authority: "I'm the CEO calling".
  - Intimidating: "Unblock this website, or I'll call the manager".
  - Giving urgency: "I have to complete this transaction today".
  - Showing trust: "I know you, and I'm depending on your good will".
- It is also used as influence campaigns to sway attention and sympathy in a particular direction:

  (Video 2:32, How Cambridge Analytica Exploited the Facebook Data of Millions | NYT)

Psychological Approaches

Social engineering psychological approaches often involve:

- Impersonation: the attacker may pretend to be an employee calling the IT support for help.
- Phishing: the attacker sends an email to trick the user into providing private information such as passwords, bank account numbers, etc.
- Variations on phishing attacks:
  - Spear phishing: targets specific users.
  - Whaling: targets wealthy individuals or executives in higher positions.
  - Vishing: uses phone calls instead of emails.
  - Smishing: uses texting or short message services (SMS).

(Video 2:58, Watch this hacker break into a company)

(Video 6:16, Hacking challenge at DEFCON)

Psychological Approaches

- Redirection: the attacker directs a user to a fake site that looks like the original site but is filled with ads so the attacker can make money from the generated traffic (amozon.com instead of amazon.com).
- Spam: the attacker sends an unsolicited email to a large number of recipients. Usually, the attacker advertises a fake or overpriced product, if few recipients respond, the profit is huge.
- Hoax: the attacker sends a false warning (e.g., a malware was found in your system) and asks the user to act (delete files or change configurations).
- Watering hole: the attacker targets a smaller group such as managers who visit a common website (e.g., a supplier website) and infects it with a malware that will make its way up to their computers.

Physical Approaches

Social engineering physical approaches could be:

- Dumpster diving: the attacker looks in trash to find information that can be useful in an attack.
- Tailgating: the attacker follows an employee who is authorized to enter a building and enters directly behind them when the gate is open.
- Shoulder surfing: the attacker observes someone entering secret information, such as a password to log in or the PIN number on an ATM keypad.

Question

- An attacker crafts a phishing email targeting the employees in the accounting department. It tells the employee that their account was breached, and they need to change their password by following a link in the email. Which of the following is the best to describe this email?
  - Spear phishing.
  - Smishing.
  - Spam.
  - Watering hole.
  - Whaling.

The End

End of Slide Set