Classifying Cybersecurity Threats

Characteristics that differentiate the types of cybersecurity threat actors.

- **Internal vs External**
- **Level of Sophistication/Capability**
- **Resources/Funding**
- **Intent/Motivation**

Hats that the hackers wear

- **White-hat hackers**
  Those who act with authorization and seek to discover security vulnerabilities with the intent of correcting them.
- **Black-hat hackers**
  Unauthorized attackers, those with malicious intent.
- **Gray-hat hackers**
  Semi-authorized attackers, are those who fall somewhere between white and black hat hackers.
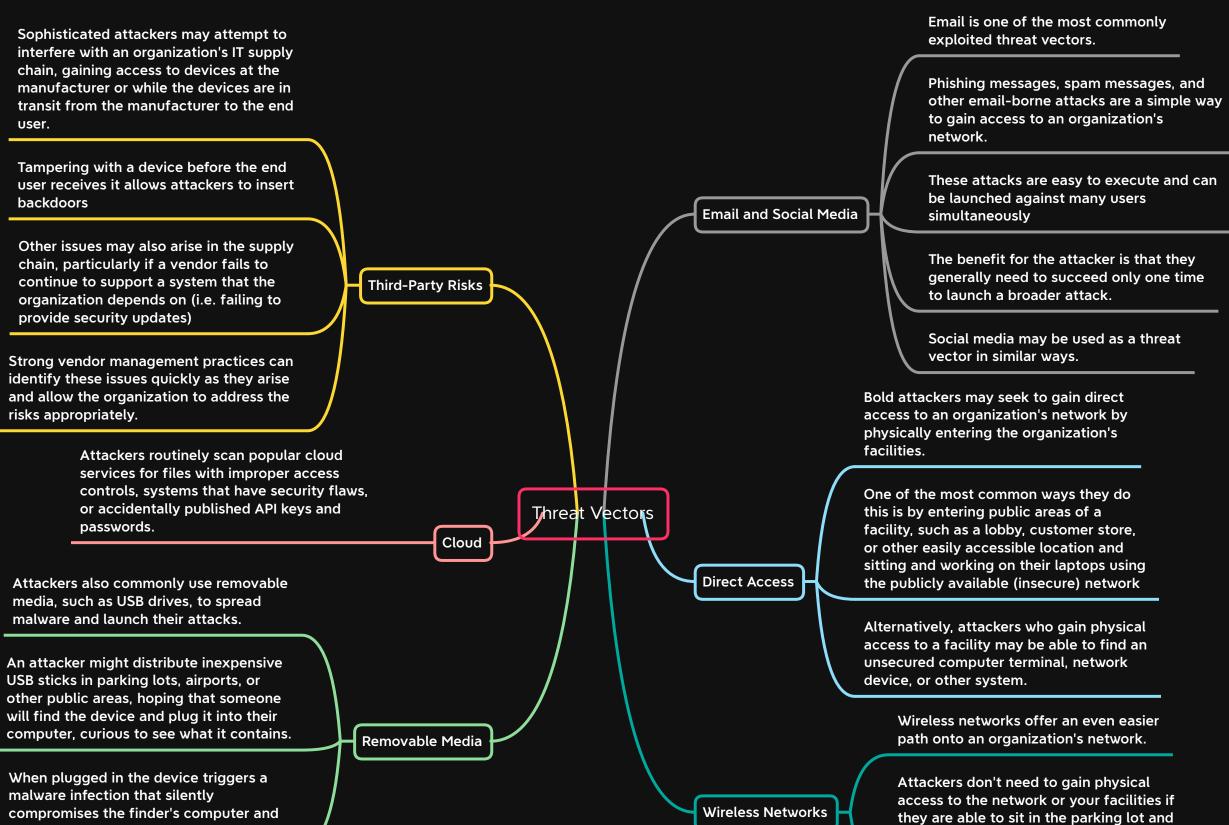
Zero-day attacks are attacks that exploit zero-day vulnerabilities which are vulnerabilities that are newly discovered and thus unknown to the public

Shadow IT
is the act of intentionally or unintentionally putting sensitive information in the hands of vendors outside of the organization's control.

Threat Actors

Competitors
- Competitors may engage in corporate espionage designed to steal sensitive information from your organization and use it to their own business advantage.

Insiders
- Insider attacks occur when an employee, contractor, vendor, or other individual with authorized access to information and systems uses that access to wage an attack against the organization.
- These attacks are often aimed at disclosing confidential information, but insiders may also seek to alter information or disrupt business processes.
- An insider might be of any skill level and also might have differing motivations behind their attacks.
- An insider will usually be working alone and have limited financial resources and time. However, the fact that they are insiders gives them an automatic advantage.
- Behavioral assessments are a powerful tool in identifying insider attacks.
- Cybersecurity teams should work with human resources partners to identify insiders exhibiting unusual behavior and intervene before the situation escalates.

Script Kiddies
- Term for people who use hacking techniques but have limited skills.
- Often such attackers may rely almost entirely on automated tools they download from the Internet.
- These attackers often have little knowledge of how their attacks actually work, and they are simply seeking out convenient targets of opportunity.
- There are 2 reasons why even though script kiddies don't know much about hacking posses a threat
  - Simplistic hacking tools are freely available on the Internet.
  - Script kiddies are plentiful and unfocused in their work (i.e. they have no specific targets they focus on anyone)
- These individuals tend to be rather young, they work alone, and they have very few resources.

Advanced Persistent Threats (APTs)
- State actors hacking into either foreign governments or corporations.
- They use advanced techniques
- The attacks are persistent, occurring over a significant period of time (Maybe years)
- They tend to be characterized by highly skilled attackers with significant resources.
- The motive can be political or economic.
- In some cases, the attack is done for traditional espionage goals: to gather information about the target's defense capabilities.
- In other cases, the attack might be targeting intellectual property or other economic assets

Criminal Syndicates
- The ranks of cybercriminals include links to traditional organized crime families in the United States, outlaw gangs, the Russian Mafia, etc..
- The common thread among these groups is motive and intent. The motive is simply illegal financial gain. They simply want to generate as much illegal profit as they possibly can.
- Cyber crime categories that they are active in
  - Cyber-dependent crime, including ransomware, data compromise, distributed denial-of-service (DDoS) attacks, website defacement, and attacks against critical infrastructure
  - Child sexual exploitation, including child pornography, abuse, and solicitation
  - Payment fraud, including credit card fraud and business email compromises
  - Dark web activity, including the sale of illegal goods and services
  - Terrorism support, including facilitating the actions of terrorist groups online
  - Cross-cutting crime factors, including social engineering, money mules, and the criminal abuse of cryptocurrencies
- Organized crime tends to have attackers who range from moderately skilled to highly skilled (Rarely script kiddies and if they exist they are caught quickly)
- Organized crime groups tend to have more resources, both in terms of time and money, than do hacktivists or script-kiddies.

Hacktivists
- Hacktivists use hacking techniques to accomplish some activist goal.
- They might deface the website of a company whose policies they disagree with or attack a network due to some political issues
- They believe that they are motivated by the greater good, even if their activity is illegal
- They may view being caught as a badge of honor and a sacrifice for their cause.
- The skill levels of hacktivists vary widely. Some are only script kiddies, whereas others are quite skilled, having honed their craft over the years.
- The resources of hacktivists also vary somewhat. Many are working alone and have very limited resources. However, some are part of organized efforts.
- Example: Anonymous

Threat Vectors

Third-Party Risks
- Sophisticated attackers may attempt to interfere with an organization's IT supply chain, gaining access to devices at the manufacturer or while the devices are in transit from the manufacturer to the end user.
- Tampering with a device before the end user receives it allows attackers to insert backdoors
- Other issues may also arise in the supply chain, particularly if a vendor fails to continue to support a system that the organization depends on (i.e. failing to provide security updates)
- Strong vendor management practices can identify these issues quickly as they arise and allow the organization to address the risks appropriately.

Cloud
- Attackers routinely scan popular cloud services for files with improper access controls, systems that have security flaws, or accidentally published API keys and passwords.

Removable Media
- Attackers also commonly use removable media, such as USB drives, to spread malware and launch their attacks.
- An attacker might distribute inexpensive USB sticks in parking lots, airports, or other public areas, hoping that someone will find the device and plug it into their computer, curious to see what it contains.
- When plugged in the device triggers a malware infection that silently compromises the finder's computer and places it under the control of the attacker

Email and Social Media
- Email is one of the most commonly exploited threat vectors.
- Phishing messages, spam messages, and other email-borne attacks are a simple way to gain access to an organization's network.
- These attacks are easy to execute and can be launched against many users simultaneously
- The benefit for the attacker is that they generally need to succeed only one time to launch a broader attack.
- Social media may be used as a threat vector in similar ways.

Direct Access
- Bold attackers may seek to gain direct access to an organization's network by physically entering the organization's facilities.
- One of the most common ways they do this is by entering public areas of a facility, such as a lobby, customer store, or other easily accessible location and sitting and working on their laptops using the publicly available (insecure) network
- Alternatively, attackers who gain physical access to a facility may be able to find an unsecured computer terminal, network device, or other system.

Wireless Networks
- Wireless networks offer an even easier path onto an organization's network.
- Attackers don't need to gain physical access to the network or your facilities if they are able to sit in the parking lot and access your organization's wireless network.