Chapter 2 Cybersecurity Threat Landscape

# Classifying Cybersecurity Threats

* Internal vs. External
* Resources/Funding
* Intent/Motivation

White hat hackers have permission. Black hat hackers don’t. Grey hats are semi-authorized.

Zero-Day Attacks: a cyberattack that exploits software, firmware, or hardware vulnerability before a patch is available

## Threat Actors

### Unskilled Attackers

Also known as Script Kiddie, unskilled and mostly rely on automated tools. There are simplistic hacking tools free on the internet. There are a lot and are unfocused. They are trying to prove their skill. Being unfocused is dangerous as they will try to do as much as possible in as many places as possible. Not a lot of skill and resources.

### Hacktivist

Hack as a form of protest. Always has a purpose. Does not mind getting caught. Works alone or with a group. Skill levels vary as well as resources.

### Organized Crime

Goal is to hack for money. Rather not get caught. Skills go from moderate to very skilled. Can have lot of resources.

### Nation-State Attackers

Advanced Persistent Threats (APTs): Describes a series of attacks that they first traced to sources in the Chinese military. High skill, a lot of resources, does not want to get caught. Goal is for attacks to last for years.

### Insider Threat

An attack from the inside. Skill level varies. Limited financial resources, but a lot of resources as it Is from the inside.

### Competitors

May engage in corporate espionage designed to steal sensitive information from organizations to give your organization an advantage.

### Attacker Motivation

* Data Exfiltration: Attacks are motivated by obtaining sensitive information.
* Espionage: Attacks motivated by organizations seeking to steal secret information from another organization.
* Service Disruptions: Attacks that interrupt critical systems or networks.
* Blackmail: Extort a victim by the threat of leaking sensitive information.
* Financial Gain: Attacks to gain money.
* Philosophical / Political beliefs: Attacks motivated by an ideology or a political reason.
* Ethical / White hat hacking: Attacks to help improve security.
* Revenge: Attacks desired by getting even with an individual or organization.
* Disruption / Chaos: Attacks desired to cause chaos in the day-to-day functions.
* War: Military or civilian groups disrupting another army in hopes to win a war.

## Threat Vectors and Attack Surfaces

Attack Surface: Finding a vulnerability in a system or application to exploit.

Threat Vectors: The means that a threat actor uses to obtain access via Attack Surface.

### Message-Based Threat Vectors

* Emails 🡪 phishing messages and spam
* Text
* Voice calls 🡪 vishing
* Social media

### Wired Network

Attacks by having a physical connection (wire) to the victim.

### Wireless Networks

Attacks that use a Bluetooth connection or a Wi-Fi connection.

### Systems

The operating system may have bugs, expose ports, or no longer support by vendors.

### Files and Images

Sending a file that contains or hides malicious code.

### Removable Devices

Using removable media (USB) to spread malware.

### Cloud

Looks for cloud services with flaws or publicly known API keys and passwords.

### Supply Chain

Tampering with devices when the hardware is with the vendor or with the end user. Inserting vulnerabilities into software before it is released/deployed. Vendors fail to continue to support a system which can cause loss of security.

# Threat Data and Intelligence

Are resources that can be used to learn about changes in the threat environment. Intelligence can be used by predictive analysis to find potential risks.

**Vulnerability databases:** Reports of vulnerabilities and provide insight into types of exploits being discovered by researchers.

**Indicators of Compromise (IoCs):** Telltale signs an attack has taken place (file signatures, log patterns, and other evidence left behind from the attacker) and can also find files and code repositories that offer threat intelligence information.