

## **THREAT ACTORS**

### **Introduction**

In this lesson, we'll be looking at some common types of threat actors. We'll discuss some of their attributes, and what makes them unique or dangerous. In general, we'll start with less dangerous types of threat actors, and move on to more dangerous types.

Before we begin, let's talk about a type of threat actor we won't be going over: Individual Hackers. Hackers are people too, and they have widely varied personalities, motivations, and skill sets. There is no single profile that can fit all individual hackers without being incredibly vague. Generally speaking, hackers are categorized into ethical (white-hat), malicious (black-hat), and semi-ethical (gray-hat) depending on the actions they take.

We also won't be discussing APTs (Advanced Persistent Threats) as a type of their own: An APT is simply a threat actor that has advanced capabilities and is difficult to dissuade. If it takes 6 months to compromise a target, then they'll spend 6 months working on it.



---







## Human Error

One of the most common threat actors isn't some shadowy hacker group, but the potential to make mistakes that lies in every one of us! Even though these mistakes aren't intentionally malicious, they still represent an (abstract) threat actor that should be considered when designing systems. Human error doesn't have any specific targets or objectives - it can strike anytime and anywhere that humans are involved, "attacking" through unpredictable means and with unpredictable results.

Protecting against **human error** means designing processes and systems in ways where it is impossible (or at least *very* difficult) for mistakes to have a serious impact. We see this in Murphy's Law: if it's possible to do something incorrectly, someone *will* do it incorrectly. Human error has caused data

breaches, civil engineering disasters, airplane crashes, industrial accidents, and much, much more.

Human error can be both external and internal and includes any action that can be done by a human. Human error has whatever access has been granted to the human making the error, but very little sophistication. For example, multi-step mistakes are less likely than very simple errors. Human error has no specific targets, as well as no "negative" motivation, as the humans making the errors are often trying NOT to make errors!

|  |   |                       |
|--|---|-----------------------|
| Name:<br><b>Human Error</b>  | Threat Source:<br> <b>Internal</b><br>&<br> <b>External</b> | Goals:<br><b>None</b> |
| Sophistication:<br><b>Very Low</b><br> | Resources:<br><b>Varies</b><br>  |                       |
| Motivation:<br><b>None</b><br>        | Support:<br><b>None</b><br>   |                       |
| Notes:<br><b>Human error, while not malicious, is still a potential threat.</b>  |   |                       |

---

## Script Kiddies

**Script Kiddies** is a term that refers to inexperienced hackers who lack experience, as well as have a low understanding of [hacking](#) and the tools used to do it. They make use of already existing hacking tools and scripts, without understanding the underlying vulnerabilities that are being exploited. The word "kiddie", usually used to refer to a small child, is instead used to represent their lack of sophistication.

Script kiddies are usually opportunistic in their targeting, and often hack just for the sake of hacking, rather than achieving some premeditated objective.

However, this lack of planning or high-level motivation doesn't mean script kiddies are harmless!

Modern hacking tools are easy to acquire, configure, and use, and *the vast majority of vulnerabilities that get exploited in real-world scenarios are known vulnerabilities for which exploits have been developed and distributed.*

Script kiddies are almost always external threats, with low sophistication and resources. They often have minimal or no funding, and only freely available resources. Their goals can vary, but they usually operate opportunistically and don't have a great deal of motivation. Once a script kiddie has been stopped by security measures, they're likely to move on to an easier target.

|  |   |                                |
|--|---|--------------------------------|
| Name:<br><b>Script Kiddies</b>                                 | Threat Source:<br><div>• <b>External</b></div>  | Goals:<br><b>Opportunistic</b> |
| Sophistication:<br><div><div></div></div> <b>Low</b>           | Resources:<br><div><div></div></div> <b>Low</b> |                                |
| Motivation:<br><div><div></div></div> <b>Low</b>               | Support:<br><div><div></div></div> <b>Low</b>   |                                |
| Notes:<br><b>Typically inexperienced and easily dissuaded.</b> |   |                                |

---

## Insider Threats


**Insider threats** are threat actors operating *within* an organization. Insider threats are usually employees but contractors or ex-employees can be considered insider threats too.

Insider threats can have a variety of goals, such as financial gain, personal grievances, or gaining some sort of advantage over others. Insider threats can operate opportunistically or deliberately, sometimes working with other threat actors to give them access they would not have otherwise had.

*Insider threats usually have elevated access and increased knowledge when compared to external threat actors. This can make them more difficult to detect, and it can give them more options for how to attack the organization. Insider threats can have a wide range of sophistication - A disgruntled cashier, for example, will probably not be as sophisticated a threat as a disgruntled security analyst.*

Insider threats are one reason why it's so important to follow the principle of least privilege! *Limiting the access insiders have means that a malicious insider will have fewer options available to them, and can do less damage.*

One specific type of insider threat is that of Shadow IT. **Shadow IT** refers to assets that are part of an organization's network, but aren't set up or managed by IT AND that IT and Security are not aware of. This can be dangerous since unknown assets on an organization's network can create attack vectors that the organization is not aware of until it's too late.

|   |   |   |
|---|---|---|
| Name:<br><b>Insider Threats</b>   | Threat Source:<br> <b>Internal</b> | Goals:<br><b>Personal gain, revenge, varies</b> |
| Sophistication:<br><b>Varies</b><br><input type="text"/>                                      | Resources: <b>Elevated access to internal assets</b><br><div><div></div></div>  |   |
| Motivation:<br><b>Varies</b><br><input type="text"/>  | Support:<br><b>Varies</b><br><input type="text"/>   |   |
| Notes:<br><b>A malicious IT admin would be a lot more dangerous than a malicious cashier.</b> |   |   |

---

## Hacker Groups

Before we move on to "scarier" threat actors, we need to discuss the generic concept of a "hacker group". **Hacker groups** are, as the name suggests, groups of hackers. This is a very broad term, and it can refer to everything

from a group of friends who like tinkering with game consoles to state-sponsored threat groups.

Many of the types of threat actors we will soon discuss also operate as groups, but there are plenty of groups that don't fit cleanly into any one category. These "leftover" groups can have a staggering variety of sophistication, resources, goals, and motivations, without necessarily having a clearly defined set of tactics.

One hacker group might be for people interested in [hacking](#) Bluetooth devices, for example, while another group might be loosely-knit groups of individuals, all with their own style, who like to show off their work to each other.

Some groups might operate opportunistically, while others might focus on a specific target with a long-term objective in mind, though these objectives aren't always "reasonable". There has been at least one documented case of a hacker group compromising a game developer because... well, they just wanted to play an early version of an upcoming game.

|  |   |  |
|--|---|--|
| Name:<br><b>Hacker Groups</b>  | Threat Source:<br><div><div></div><b>External</b></div> | Goals:<br><b>Varies</b>                    |
| Sophistication:<br><b>Varies</b> *Usually high or less<br><div><div></div></div> |   | Resources:<br><b>Varies</b><br><div></div> |
| Motivation:<br><b>Varies</b><br><div></div>                                      |   | Support:<br><b>Varies</b><br><div></div>   |
| Notes:<br><b>This type is a real wildcard, huh?</b>                              |   |  |

---

## Hacktivists

**Hacktivists** are hackers with an ideology, who strongly believe in a cause and are willing to break the law to further that cause.

Hacktivists are defined by their strong motivation; this motivation means that they can be *very difficult to dissuade from a target*. If one method doesn't work, they will just try different approaches until something works.

Hacktivists can have a wide variety of objectives that they aim to achieve via [hacking](#). Defacement, denial of service, and leaking confidential information are all common actions taken by hacktivists.

Hacktivists are usually external threats, and they can have a range of sophistication and resources. Their goals are usually in service to whatever cause they are rallying behind. The most dangerous aspect of hacktivist groups is their motivation. Many of these groups have goals that seem noble on paper. For example, revealing corruption or freeing someone being held against their will by an ethically dubious hospital, and it can be easy to see why these hackers would feel strongly enough to take matters into their own hands.

|  |  |                                     |
|--|--|-------------------------------------|
| Name:<br><b>Hacktivists</b>  | Threat Source:<br><div>• <b>External</b></div>           | Goals:<br><b>Supporting a cause</b> |
| Sophistication: <b>Usually Moderate</b><br><div><div></div></div>  | Resources: <b>Low-Moderate</b><br><div><div></div></div> |                                     |
| Motivation: <b>Very High</b><br><div><div></div></div>   | Support: <b>Low-Moderate</b><br><div><div></div></div>   |                                     |
| Notes:<br><b>Highly motivated by their belief in their cause, but not willing to cause the same level of harm as cyber-terrorists.</b> |  |                                     |

---

## Competitors

Corporate espionage has existed since at least the 1700s, and the digital era has made it easier than ever for unscrupulous organizations to steal trade secrets or sabotage rivals in order to gain an unfair advantage. **Competitors** have been trying to steal secrets from others for centuries.

Corporate espionage is usually illegal, so organizations that engage or attempt to engage in it will likely focus on secrecy and deniability. This means that the tactics they use will probably be more sophisticated than usual, in an attempt to evade detection and attribution. Additionally, corporations often have large pools of resources (financial, personnel, etc) that can be leveraged by attackers on their behalf.

Most suspected cases of corporate espionage revolve around the theft (or attempted theft) of trade secrets - rival corporations probably don't have a good reason to steal a password database, for example. The threat actor's motivation is likely higher than average, as they will be focusing on competitors, but they may be unwilling to overextend and leave themselves vulnerable to detection.

Corporate espionage is primarily external but may incorporate internal elements in the form of rogue employees, or agents working for the threat actor.



|   |  |   |
|---|--|---|
| Name:<br><b>Competitors</b>   | Threat Source:<br><div> <div>•</div> <div> <b>External</b><br/> <small>*may have internal assets</small> </div> </div> | Goals:<br><b>Gaining a competitive advantage</b>                        |
| Sophistication: <b>Moderate-High</b><br><div> <div></div> <div></div> </div>  |  | Resources: <b>Moderate-High</b><br><div> <div></div> <div></div> </div> |
| Motivation: <b>Moderate-High</b><br><div> <div></div> <div></div> </div>  |  | Support: <b>Moderate</b><br><div> <div></div> <div></div> </div>        |
| Notes:<br><b>Big companies can have lots of resources, but probably won't be willing to devote them all to illegal practices.</b> |  |   |

## Organized Cybercrime

**Organized cybercrime** generally has a single overarching goal: Money. Financial fraud, data theft, extortion, trafficking, and so much more. If you can think of an underhanded way to make money with computers, there's probably a group of cybercriminals doing it.

These cybercriminals usually represent an external threat, with a wide range of sophistication. Some groups might be relatively inexperienced, while others might be experienced hackers. Likewise, the resources these groups have access to can vary, but they are likely to be higher than what a single person could muster.

Cybercrime can be both opportunistic and targeted - If there's a way for them to make money, they'll probably start taking advantage of it sooner or later. Here's a brief list of some things one group, named REvil, did in 2020 and 2021:

- Stole A terabyte of data from a law firm, then attempted to extort, among others, Madonna and Lady Gaga.
- Attacked a trust that ran schools in the UK, and held stolen data for ransom, along with student's coursework.

- Stole plans for upcoming Apple products and tried to hold them for ransom.
- Attacked a meatpacking company with [ransomware](#), extorting 11 million dollars in bitcoin.
- Targeted an energy company with ransomware.
- Stole documents from a Florida-based military contractor.

|  |  |  |                        |
|--|--|--|------------------------|
| Name:<br><b>Organized Cybercrime</b>   |  | Threat Source:<br><div>•</div> <b>External</b>       | Goals:<br><b>Money</b> |
| Sophistication: <b>Moderate-High</b><br><div><div></div></div>                     |  | Resources: <b>Moderate</b><br><div><div></div></div> |                        |
| Motivation: <b>Varies</b><br><div></div>   |  | Support: <b>Varies</b><br><div></div>                |                        |
| Notes:<br><b>Usually just in it for the money, but still a significant threat.</b> |  |  |                        |

---

## Cyber Terrorists

**Cyber terrorists** seek to use [hacking](#) to cause large-scale destruction and harm. In some ways, they can be thought of as extremist hacktivists, who seek to use intimidation and destruction to further their cause.

While cyber terrorists are unlikely to be working alone, they may lack easy access to resources. That being said, world governments have a history of covertly funding terrorist groups so there's no reason to suspect that the same couldn't be true for cyber terrorists.

Cyber terrorists are likely to target systems that would cause significant damage or loss of life if compromised: Digital or physical infrastructure such as backbone routers, power plants, water treatment plants, hospitals, etc.

|  |   |   |
|--|---|---|
| Name:<br><b>Cyber Terrorists</b>   | Threat Source:<br><div> <div>•</div> <div>External</div> </div> | Goals:<br><b>Causing large-scale destruction and harm</b> |
| Sophistication: <b>Moderate-High</b><br><div> <div></div> <div></div> </div>   |   | Resources: <b>Varies</b><br><div></div>                   |
| Motivation: <b>Very High</b><br><div> <div></div> <div></div> </div>   |   | Support: <b>Varies</b><br><div></div>                     |
| Notes:<br><b>Can have similar motivations to hacktivists, but willing to cause wide-spread harm to accomplish their goals.</b> |   |   |

---

## State Actors

**State actors** are some of the most dangerous types of threat actors. They are often highly sophisticated and work with the support of other governmental organizations. They have large quantities of resources provided to them by their government, allowing them to employ skilled hackers, not only to conduct attacks, but to search for vulnerabilities to develop into cyberweapons.

State actors are also highly motivated, working on behalf of a nation-state. If they decide to target an individual or organization, they have a specific objective in mind and will work very hard to complete that objective while remaining undetected, even in the face of adversity. Failure or detection might cause them to retreat, but likely won't dissuade them from their objective.

State actors' motivations are based on what benefits the state they work for. They may attempt to spy on foreign nations, conduct cyber warfare, defend their nation against other threat actors, spy on journalists, or whatever else the state commands of them.

State actors are a quintessential example of an **Advanced Persistent Threat (APT)**: they have advanced capabilities and access to resources and are difficult to dissuade from their objective.

|  |   |  |
|--|---|--|
| Name:<br><b>State Actors</b>   | Threat Source:<br><div> <div>•</div> <div>External<br/>*may have internal assets</div> </div> | Goals:<br><b>The goals of their backing nation</b>                     |
| Sophistication: <b>Very High</b><br><div> <div></div> <div></div> </div>   |   | Resources: <b>Very High</b><br><div> <div></div> <div></div> </div>    |
| Motivation: <b>Very High</b><br><div> <div></div> <div></div> </div>   |   | Support: <b>High-Very High</b><br><div> <div></div> <div></div> </div> |
| Notes:<br><b>The most dangerous type of threat actor. Absolutely qualifies as an APT (Advanced Persistent Threat).</b> |   |  |

## Review

In this lesson you've learned about different types of threat actors:

- Individual Hackers
- Human Error
- Script Kiddies
- Insider Threats
- Hacker Groups
- Hacktivists
- Competitors
- Organized Cybercrime
- Cyber Terrorists

Each of these threat actors has unique Tactics, Techniques, and Procedures (TTPs) and attributes. Understanding these actors, and their motivations, will help you prevent attacks on and secure your systems.

