Understand attackers

Previously, you were introduced to the concept of threat actors. As a reminder, a **threat actor** is any person or group who presents a security risk. In this reading, you'll learn about different types of threat actors. You will also learn about their motivations, intentions, and how they've influenced the security industry.

Threat actor types

Advanced persistent threats

Advanced persistent threats (APTs) have significant expertise accessing an organization's network without authorization. APTs tend to research their targets (e.g., large corporations or government entities) in advance and can remain undetected for an extended period of time. Their intentions and motivations can include:

Damaging critical infrastructure, such as the power grid and natural resources

Gaining access to intellectual property, such as trade secrets or patents

Insider threats

Insider threats abuse their authorized access to obtain data that may harm an organization. Their intentions and motivations can include:

Sabotage

Corruption

Espionage

Unauthorized data access or leaks

Hacktivists

Hacktivists are threat actors that are driven by a political agenda. They abuse digital technology to accomplish their goals, which may include:

Demonstrations

Propaganda

Social change campaigns

Fame

Hacker types

A **hacker** is any person who uses computers to gain access to computer systems, networks, or data. They can be beginner or advanced technology professionals who use their skills for a variety of reasons. There are three main categories of hackers:

Authorized hackers are also called ethical hackers. They follow a code of ethics and adhere to the law to conduct organizational risk evaluations. They are motivated to safeguard people and organizations from malicious threat actors.

Semi-authorized hackers are considered researchers. They search for vulnerabilities but don't take advantage of the vulnerabilities they find.

Unauthorized hackers are also called unethical hackers. They are malicious threat actors who do not follow or respect the law. Their goal is to collect and sell confidential data for financial gain.

Note: There are multiple hacker types that fall into one or more of these three categories.

New and unskilled threat actors have various goals, including:

To learn and enhance their hacking skills

To seek revenge

To exploit security weaknesses by using existing malware, programming scripts, and other tactics

Other types of hackers are not motivated by any particular agenda other than completing the job they were contracted to do. These types of hackers can be considered unethical or ethical hackers. They have been known to work on both illegal and legal tasks for pay.

There are also hackers who consider themselves vigilantes. Their main goal is to protect the world from unethical hackers.

Key takeaways

Threat actors are defined by their malicious intent and hackers are defined by their technical skills and motivations. Understanding their motivations and intentions will help you be better prepared to protect your organization and the people it serves from malicious attacks carried out by some of these individuals and groups.