What Is a Cyber Threat Actor? Definition, Types, Examples | Proofpoint US

Published: 2022-07-04 · Archived: 2026-04-06 00:18:21 UTC

There are several types of threat actors. Typically, each type has a specific goal, whether it's financial, espionage or simply to destroy your data. Understanding the different types of threat actors helps you build better detection methods and investigate possible attacks.

Financially Motivated Actors

The vast majority of cyber threat actors are financially motivated, regardless of their preferred mode of attack. They may distribute banking Trojans or other forms of malware to directly steal from financial websites, or they may use phishing to steal credentials and log in to bank or brokerage accounts. Some threat actors seek to profit by stealing data and either selling it or charging money to return it. And some highly sophisticated actors make use of ransomware to lock up an organization's IT infrastructure until a payment is made.

Cyber Terrorists

Cyber terrorists can target businesses, governments, or a country's infrastructure. They are given the name for the disruption they can cause to entire communities. A cyber terrorist's goal is usually to harm a country's residents and businesses, resulting in economic and physical harm.

Advanced Persistent Threat (APT) Actors

Advanced persistent threat (APT) actors are commonly aligned with a country's government and may be backed by that government either financially, with other resources, or may even be officially a part of the government. State-sponsored threats are generally targeted and motivated by espionage, looking to support the intelligence gathering priorities of their aligned government organizations. At times, these cyber threat actors may use malware to gain access to a target's accounts or target an opposing country's infrastructure and steal information. APT actors target a variety of sectors across the globe.

Hacktivists

Hackers sometimes target governments and businesses based on opposition to their target's ideology. "Anonymous" is a popular hacktivist group made up of people from all over the world, but other hacktivists might work alone. These threat actors are generally not financially motivated, seeking to damage data or infrastructure for political reasons. They can be external or insider threats focused on performing malicious activities and disrupting normal business productivity.

Insiders

Many corporations make the mistake of trusting any activity from employees or hired contractors. For example, an insider threat could be a newly disgruntled employee or a person who purposely targets a business or government. Competitor governments or businesses pay insiders to steal intellectual property and trade secrets, but some insider threats aim to simply do damage to their employer. Insider threats have become more common in recent years, inflicting the most damage and being the most difficult to detect since they have legitimate access to infrastructure and data.

Script Kiddies

Not every threat actor is a skilled attacker. Many scripts, code repositories and malware are freely downloadable for anyone to use. These cyber threat actors are colloquially known as “script kiddies” since they usually don’t have the technical skills to code or exploit vulnerabilities. Even without coding and hacking skills, script kiddies can still harm an organization’s productivity and private data. A script kiddie can also unknowingly add malware to the environment, thinking they are downloading tools they can control.

Internal User Mistakes

Insider threats don’t always have malicious intent, but the damage they cause can be just as bad as intentionally targeting the business with an attack. Usually, unintentional damage from an insider threat is associated with phishing. External attackers send phishing emails to insiders, tricking them into opening a malicious attachment or accessing a web page that tricks a targeted employee into divulging their credentials. Because the employee has legitimate access to data, insider threat actors can reveal extensive sensitive data to an attacker.
