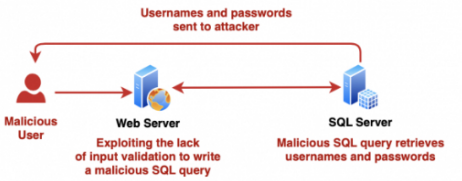
Common Threat Agents

Let's start off by discussing what threats and threat agents/actors are, then we will cover the categories that these actors are typically placed into, and research a few real-world groups and a history of their cyber attacks and operations.

WHAT ARE THREATS?

As you should remember from the **Management Principles** lesson in the **Security Fundamentals** domain, a threat is a danger that can exploit a vulnerability, resulting in a breach (impact). Below is a diagram demonstrating an intentional threat.

Intentional Threat (Hacking)

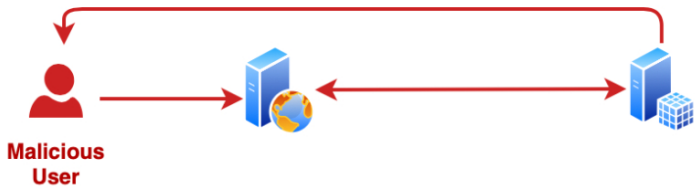


In the example above, a malicious user is exploiting a vulnerability, which is a lack of input validation (not preventing users from entering special characters into an input field, such as " / - = ` ' ") which allows the attacker to conduct a SQL injection attack, and retrieve data stored in the SQL database connected to the back-end of the vulnerable website.

- **Vulnerability:** Lack of input validation
- **Threat:** Exploiting vulnerability to write a malicious SQL query
- **Result:** Username and password tables in the database are sent to the attacker

WHAT ARE THREAT ACTORS?

A threat agent or threat actor in regard to cyber threat intelligence is an actor that intentionally or unintentionally generates an adverse effect on an organization, such as conducting a cyberattack, or unintentionally leaking information. Therefore, this can be an individual or group of individuals that cause harm in some way.



Let's use a new example. If a cybercrime syndicate hacked a server belonging to ABC Industries that suffered a remote code execution vulnerability, and managed to steal data such as user's email addresses, billing addresses, and passwords, the cybercrime syndicate (a group of individuals) would be the threat actor in this scenario, and they have caused an intentional threat, because they purposefully exploited the vulnerability and exfiltrated the data.

But not all threat actors are evil hackers or rain clouds, and sometimes threats can materialize as a result of an accident. If an employee unintentionally deletes a table in a database because they have not received proper training, then they become a threat actor themselves, despite not having malicious intentions.

- **Threat Actor:** Employee
- **Vulnerability**: Not properly trained
- **Threat:** Employee unintentionally deleting a database table
- **Result:** Missing data means application attached to database will likely not function correctly
- **Threat Type:** Unintentional = Accidental

ACTOR CATEGORIZATION

When we talk about threat actors, we are generally referring to the threat intelligence term associated with an individual or group of malicious actors that conduct cyber-dependant attacks or operations. We can generally categorize threat actors into the following 4 groups:

Cyber Criminals

This group includes hackers and crackers that are looking to make money from malicious and illegal activity, such as cyber attacks, ransomware, and phishing. The skill level can vary dramatically within this group, for example you could see a really experienced hacker classed as a cyber criminal threat actor, but you could also see a "script kiddie" in the same group, which is a term used to describe an inexperienced individual that is dependent on pre-built tools and scripts, and generally has a low level of technical knowledge.

Nation-States

These are hackers or hacking teams that work for governments around the world, and have a very high level of technical sophistication as well as resources, making them some of the most advanced adversaries out there. They typically conduct prolonged covert cyber operations, staying undetected for long periods of time whilst they silently complete any objectives they have in the target network. Nation-States are often referred to as Advanced Persistent Threats (APTs).

Hacktivists

Individuals or groups placed into this category are typically socially or politically motivated, and use cyber attacks as a way to express their views and beliefs. Hacktivists usually conduct distributed denial of service (DDoS) attacks that take systems offline by overloading their resources causing them to crash. Another common attack conducted by actors in this group is website defacement, the act of changing the content on a website's homepage to display a message or image created by the attack, usually to make a statement related to social or political views.

Insider Threat

Individuals classed into this group have intentionally or unintentionally abused their power and knowledge of an organization they work at in order to leak confidential information. Intentional cases can include disgruntled employees that are taking revenge against the company, and unintentional cases can include employees accidentally emailing documents to the wrong email address, or falling victim to a social-engineering attack.

REAL-WORLD THREAT ACTORS

In this section, we will look at two real threat actors from the nation-state and hacktivist classification groups.

- **Nation-States –** APT29 (Mandiant), also known as Cozy Bear (CrowdStrike), is a nation-state hacking group believed to be associated with Russian intelligence. This group is extremely well resourced, and constantly develop their own advanced malware to covertly complete cyber operations. APT29 was behind a spear-phishing attack against the Pentagon in 2015 that led to the organization shutting down non-classified email and internet access whilst they investigated the attack. This group has been compromising diplomatic organizations and governments since around 2010, and were believed to have been shut down in 2017, however recent activity shows that they simply developed more advanced tools and malware so that they haven't been detected.

- **Hacktivists –** Most people that are interested in information technology, or cybersecurity, have heard of the famous hacking group "Anonymous" which conducts attacks based on social and political motives. On January 19th, 2012, Anonymous conducted "Operation Megaupload" in response to the shutdown of the file sharing site Megaupload as well as anger at the House of Representatives' Stop Online Piracy Act and the Senate's Protect Intellectual Property Act. This operation included sustained distributed denial of service attacks against high-profile websites including the United States Department of Justice, and the United States Copyright Office. You can read more about Operation Megaupload in this Forbes article.

CONCLUSION

Knowing our enemy can help us to better defend our systems. By giving names to malicious actors we can better share intelligence and IOCs related to them through free, paid, and private sharing methods. This can allow defenders to create detection rules that can identify malicious activity and either block it, or alert security analysts to investigate.

Previous Topic
Mark Complete
Next Topic
Back to Lesson