The cyber threat landscape part 2: Threat actors and their motivations

BY INTIGRITI · NOVEMBER 13, 2024 · LAST UPDATED ON APRIL 28, 2025

Today, the cybersecurity threat landscape is a mixed bag of attackers with different talents, interests and creativity. Threat actors span from amateur script kiddies to state-sponsored attackers, and each present their own set of challenges for organizations trying to secure their digital perimeter. This blog will dive into different capabilities of threat actors today, what motivates them, and resources at their disposal.

But how can organizations replicate the way threat actors hunt for vulnerabilities? We'll get to this later in the blog.

1. Script kiddies: Lesser skilled but still dangerous

The title 'script kiddie' is often considered the lowest level of skill and experience among cyber attackers. A script kiddie is a person who uses pre-packaged scripts, maybe tools and exploits created by others to launch attacks. Normally, they are not able to develop malware with complex functions or perform precision attacks. However, if you can buy the best exploit toolkit, all of a sudden the resources accessible today can largely increase the capability of script kiddies.

Script kiddies usually attack targets of opportunity. This means exploiting commonly known vulnerabilities that organizations have not patched or misconfigurations in any popular software. Their tactics can extend from site defacements to causing minor disturbances by launching distributed denial-of-service (DDoS) attacks. Script kiddies are dangerous due to the real financial and reputational damage they can do, especially for companies who have unpatched systems or weak defenses.

2. Insiders: The threat from within

Insider threats come from individuals within an organization who misuse their access to sensitive information. Unlike external attackers, insiders already possess legitimate access to systems and data, making them especially dangerous and difficult to detect. These individuals could be current or former employees, contractors, or third-party vendors. Insider threats are often categorized into two types: malicious and unintentional.

Malicious insiders intentionally exploit their access to steal data, sabotage systems, or facilitate other attacks, often motivated by personal grievances, financial incentives, or collaboration with external threat actors. Unintentional insiders, on the other hand, may accidentally leak information or click on a phishing link, inadvertently opening the door to cyber attackers. Insider threats are challenging because they blur the line between user and attacker, making detection and prevention particularly difficult without stringent monitoring.

3. Hacktivists: Driven by ideology

Hacktivists are cyber attackers motivated by social or political causes. They often see themselves as digital activists, using cyber tactics to promote their agendas or challenge perceived injustices. Hacktivist groups typically target government agencies, large corporations, and organizations they view as unethical or oppressive, with their attacks varying widely in severity and scope.

Common hacktivist tactics include website defacement, DDoS attacks, and data leaks aimed at damaging reputations, disrupting services, or bringing public attention to a cause. Hacktivist campaigns are generally opportunistic, leveraging well-known vulnerabilities or simple attack methods to achieve maximum visibility and impact. While hacktivists are often not as technically sophisticated as APTs, their attacks can still cause significant reputational harm and financial loss.

4. Cybercriminals: Profit-driven attackers

Unlike script kiddies, most cybercriminals have the technical skills needed to develop and deploy their own malware, execute phishing campaigns, and conduct complex social engineering schemes. Their motivation? Money.

Small and medium-sized businesses are a frequent target as many do not have the resources to defend themselves from cyberattacks. However, large corporations should in no way be considered beyond reach, and weekly news on latest breaches reminds us just how real this type of threat actor is when it comes to enterprise organizations.

Cybercriminals operate across online marketplaces and the dark web, selling stolen data, malware kits, and hacking tools to other criminals. By leveraging tactics such as phishing, ransomware, and data exfiltration, cybercriminals have created a sophisticated economy that trades in data and exploits. Their attacks can be highly targeted or broad in scope, but they are almost always financially motivated and often disruptive.

4. Advanced Persistent Threats (APTs): Strategic, long-term threats

Advanced Persistent Threats (APTs) are among the most sophisticated and dangerous types of cyber actors, often backed by state sponsors or well-funded organizations. APTs conduct prolonged, targeted campaigns designed to infiltrate a specific organization or sector and remain undetected for extended periods. Their goals are typically strategic, including cyber espionage, intellectual property theft, and infrastructure sabotage.

APTs utilize highly advanced techniques to evade detection, often using custom-built malware, zero-day exploits, and multi-stage infiltration strategies. They may take months or even years to establish their presence, stealthily moving through systems to exfiltrate data or compromise sensitive assets. APTs are difficult to detect and combat due to their stealth, resource backing, and persistence. Because of this, a strong bug bounty program can be an effective tool for identifying vulnerabilities APTs might exploit, enabling proactive defense measures.

6. Nation-state cyberattacks: Highly resourced and often undetectable

Nation-states represent the highest level of threat actor in terms of resources, capabilities, and intent. State-sponsored attackers are often well-funded, with access to extensive resources and infrastructure. Their motives are usually political or strategic, focusing on economic advantages, espionage, or disruption of rival nations. These actors often target critical infrastructure, government agencies, financial systems, and essential services like healthcare and energy, as these are areas where attacks can inflict maximum societal and economic harm.

Nation-states can launch tailored attacks designed for specific targets, often using zero-day vulnerabilities and highly covert techniques. Their actions are often complex, involving sophisticated tools and techniques that challenge even the most advanced defenses.

The role of bug bounty programs in combating diverse threats

As we can see, each of these cyber threat actors pose unique challenges that require layered defensive measures. Outdated security models that protect against only low-level threats are no longer sufficient.

Which brings us back to the question at the start of this blog: How can organizations replicate the way threat actors hunt for vulnerabilities?

You beat the threat actors at their own game.

Bug bounty programs were created for exactly this purpose – to channel the same drive and creativity for hacking into a force for good, motivating and rewarding ethical hackers (also known as security researchers) to find and fix issues first, before vulnerabilities can be exploited.

Script kiddies can exploit simple, well-known vulnerabilities, but a bug bounty hunter can ensure these are quickly identified and patched.

Insider threats are trickier, but researchers can identify misconfigurations or weak access controls that might make insider actions easier to execute or harder to detect.

Hacktivists may target a company's public-facing applications. Researchers help identify and mitigate these weaknesses, reducing the risk of damaging attacks.

Cybercriminals are financially motivated, but proactive vulnerability detection with the help of a global community of security experts helps prevent ransomware, phishing, and data theft by finding potential entry points first.

APTs thrive on staying hidden, but a bug bounty program harnesses the creativity of the crowd, enabling organizations to better discover subtle vulnerabilities before they can be exploited in these long-term campaigns.

Nation-state actors and cyber terrorists are sophisticated and well-resourced, making it critical to preemptively address vulnerabilities that could serve as entry points for strategic attacks.

The above are only examples of ways organizations bringing new capabilities to their security defense – attackers will use every resource, creative hack and new innovation to achieve their motivations. Shouldn't your security strategy harness the same level of ingenuity and intelligence to defend against them?

A call to action: Be proactive with bug bounty programs

The threat environment is becoming more and more complex. A proactive approach to cybersecurity is not just beneficial—it's essential. Bug bounty programs empower organizations to preemptively identify and fix vulnerabilities across their systems, providing a flexible, scalable, and cost-effective solution to defend against a diverse range of cyber threat actors. Because even with the best in-house security teams, budget constraints can limit the scope of security testing and vulnerability detection. The collective creativity of thousands of ethical hackers is far more effective at uncovering security gaps than any single team alone.

Unlike traditional security measures, bug bounty programs harness a global network of elite cybersecurity experts who leverage cutting-edge tools and insights to simulate sophisticated attacks—replicating the methods of all different types of threat actors. With real-world testing environments and dedicated support, bug bounty hunters are empowered to find and report vulnerabilities that others miss, giving your business the ultimate advantage to discover and fix critical security gaps before they can be exploited.

In this era of heightened cyber risk, investing in a bug bounty program is one of the most effective ways to safeguard against the growing and varied array of cyber threats.

If you're ready to learn more about bug bounty and our pay-for-impact approach, have a chat with one of our experts today.