Talence Security

Cybersecurity Adversaries Profiles Cheat Sheet

Most Dangerous

Adversary Profile	Description	Motivation	Tactics	Impact	Skill Level	Example
Nation-State Actors	Government-sponsored groups conducting espionage or sabotage.	Intelligence gathering, geopolitical goals.	Advanced TTPs, zero-day exploits, supply chain attacks, sophisticated malware like Stuxnet.	Widespread disruption, intellectual property theft, national security risks.	★★★★★	APT29 (Russia), APT41 (China) engaging in cyber espionage.
Cybercriminals	Organized criminals focused on financial gain through cyber means.	Profit, financial gain.	Ransomware attacks, phishing, online fraud, extortion.	Financial loss, data theft, operational disruption.	★★☆☆☆ ★★★★☆	Ransomware groups like LockBit or ALPHV demanding ransom.
Insiders	Employees or contractors misusing their access for malicious purposes.	Financial gain, revenge, coercion.	Data theft, sabotage, espionage, leaking confidential information.	Often severe due to access to sensitive information.	★★★☆☆	Edward Snowden leaking classified NSA information.
Corporate Espionage	Companies spying on competitors to gain an advantage.	Corporate gain.	Phishing, insider threats, bribery, cyber infiltration.	Loss of competitive advantage, financial loss, IP theft.	★★★★☆	Hiring hackers to steal trade secrets from competitors.
Cyber Mercenaries	Hackers offering services to the highest bidder.	Profit-driven.	DDoS attacks, ransomware deployment, industrial espionage.	Ranges from minor disruptions to significant economic losses.	★★☆☆☆ ★★★★☆	DDoS-for-hire services or malware/exploit development sold on dark web markets.
Terrorist Groups	Extremists using cyber tactics to instill fear or disrupt infrastructure.	Religious/political extremism.	Website defacement, attacks on critical infrastructure, spreading disinformation.	Potential to disrupt critical services, cause panic, spread propaganda.	★★☆☆☆	Targeting power grids or financial systems.
Hacktivists	Politically/socially motivated attackers disrupting operations they oppose.	Ideological, political, social causes.	Website defacement, DDoS attacks, data leaks, doxing.	Minor disruptions to significant reputational damage.	★★☆☆☆	Anonymous targeting perceived unethical organizations.
Gray Hat Hackers (Thrill Seekers)	Hackers bypassing systems for personal challenge, sometimes without malicious intent.	Curiosity, personal challenge, ego boost.	Penetration testing-like activities, exploiting vulnerabilities for fun.	Accidental damage or exploitation by malicious actors.	★★★☆☆	A hacker exploiting vulnerabilities for fun or prestige. Researcher dropping zero-day with no responsible disclosure.
Script Kiddies	Inexperienced individuals using tools they don't fully understand.	Seeking recognition, entertainment, proving a point.	Use automated tools to exploit known vulnerabilities.	Typically low-level damage; unpatched systems are vulnerable.	★☆☆☆☆	Teenager using a botnet service for a DDoS attack.

Version 1.0
September 2024