Cybersecurity Threat Actors: Compare and Contrast

A Comprehensive Overview

Brendan Shea, PhD

March 7, 2025

Understanding the Cyber Threat Landscape: An Overview

- Cybersecurity threats have evolved significantly in complexity and impact over the past decades.
- **Threat actors** are individuals or groups who have the potential to cause harm to information systems and networks.
- The global cost of cybercrime is projected to reach $10.5 trillion annually by 2025, highlighting the importance of understanding threats.
- Modern cybersecurity requires identifying not just attack methods, but the actors behind them and their motivations.
- This knowledge enables organizations to build more effective, targeted defense strategies.

Why Study Threat Actors? The Importance of Know Your Enemy

Security Principle

Understanding who might attack you and why is fundamental to effective defense.

- Different threat actors employ different tactics, techniques, and procedures (TTPs).
- Knowing potential attackers helps prioritize defenses against the most likely threats.
- **Threat intelligence** involves gathering and analyzing information about threat actors to improve security posture.
- Defenses against nation-state actors differ significantly from those targeting opportunistic criminals.
- Early identification of threat actor signatures can dramatically reduce incident response time.

The Evolution of Cyber Threats: Past, Present, and Future

- The 1980s-1990s: Early hackers were primarily motivated by curiosity and technical challenge.
- The 2000s: Rise of financially motivated cybercrime and the formation of underground economies.
- The 2010s: Emergence of state-sponsored cyber operations and sophisticated persistent threats.
- Current landscape: Blurred lines between threat actor categories with shared tools and techniques.
- Future trends point toward more automated attacks, AI-powered threats, and increased targeting of emerging technologies.

Nation-State Actors: Government-Sponsored Cyber Operations

Key Characteristics

Nation-state actors typically have extensive resources, sophisticated capabilities, and strategic objectives aligned with national interests.

- **Nation-state actors** are government-sponsored groups that conduct cyber operations to further national interests.
- These actors typically maintain the most sophisticated and persistent attack capabilities.
- Primary motivations include espionage, critical infrastructure sabotage, and military advantage.
- Examples include APT28 (Russia), APT1 (China), Equation Group (attributed to NSA), and Lazarus Group (North Korea).
- Nation-state attacks often feature custom malware, zero-day exploits, and multi-year campaign timeframes.

Case Study: Stuxnet and Nation-State Capabilities

Background

Discovered in 2010, Stuxnet targeted Iranian nuclear centrifuges at the Natanz uranium enrichment facility.

- Stuxnet demonstrated unprecedented sophistication, using four zero-day vulnerabilities and stolen digital certificates.
- The malware was specifically designed to target Siemens industrial control systems used in uranium enrichment.
- It represented the first known case of malware designed to cause physical damage to critical infrastructure.
- Attribution points to a joint US-Israeli operation codenamed "Olympic Games."
- This case illustrates how nation-state actors can combine intelligence resources, technical expertise, and strategic patience.

Script Kiddies and Unskilled Attackers: Low Sophistication, High Impact

- **Script kiddies** are inexperienced attackers who use existing tools and exploits without understanding the underlying technology.
- Despite low sophistication, these actors can cause significant damage due to the availability of automated attack tools.
- Motivations typically include curiosity, desire for notoriety, or simple mischief rather than financial gain.
- These attackers often target vulnerable systems indiscriminately rather than focusing on specific organizations.
- The democratization of hacking tools has significantly increased the number of unskilled threat actors.

Hacktivists: When Digital Activism Meets Cyber Capabilities

Notable Example

The Anonymous collective has conducted operations against organizations they perceive as corrupt, including governments, corporations, and religious institutions.

- **Hacktivism** refers to hacking for politically or socially motivated purposes rather than financial gain.
- Hacktivist operations typically seek to bring attention to causes through website defacement, DDoS attacks, or data leaks.
- These actors often operate in loose collectives rather than rigid hierarchical structures.
- Their technical sophistication varies widely, from basic DDoS attacks to complex data exfiltration.
- Hacktivists frequently announce their campaigns publicly to maximize awareness of their cause.

The Insider Threat: Dangers from Within

- **Insider threats** come from individuals with legitimate access to an organization's systems and data.
- These actors can be current or former employees, contractors, or business partners with authorized access.
- Insider attacks are particularly dangerous because they bypass many perimeter security controls.
- Motivations include financial gain, revenge for perceived wrongs, ideological disagreements, or coercion by outside actors.
- Studies suggest insider threats are responsible for approximately 22% of security incidents but tend to be the most costly.

Organized Crime in Cyberspace: Digital Profit Centers

Business Model

Cybercriminal groups have evolved sophisticated business models including Ransomware-as-a-Service (RaaS), which allows affiliates to deploy attacks while sharing profits with the malware developers.

- **Cyber criminal organizations** operate like businesses, with hierarchical structures and specialized roles.
- Primary motivation is financial gain through ransomware, banking trojans, credential theft, and fraud.
- These groups maintain advanced technical capabilities and often recruit skilled developers and security experts.
- Modern cybercrime groups have developed sophisticated supply chains and partnerships in the criminal underground.
- Examples include groups like FIN7, Carbanak, and various ransomware gangs like REvil and DarkSide.

Case Study: Conti Ransomware Group Operations

Impact

The Conti ransomware group extorted over $180 million from victims in 2021 alone, targeting healthcare, government, and critical infrastructure.

- Conti operated a sophisticated business model with specialized teams for initial access, ransomware deployment, and negotiations.
- The group maintained a detailed wiki, help desk, and salary structure mimicking legitimate software companies.
- In 2022, an insider leaked Conti's internal communications and source code following geopolitical disagreements.
- The group leveraged "double extortion" tactics, both encrypting data and threatening to publish stolen information.
- This case demonstrates the professionalization and business-like operation of modern cybercriminal enterprises.

Shadow IT: The Accidental Threat Actor

- **Shadow IT** refers to information technology systems deployed by departments without explicit organizational approval.
- These unofficial systems often lack proper security oversight, creating vulnerabilities in the organization's security posture.
- Unlike malicious threat actors, shadow IT practitioners typically have legitimate business objectives but create risk inadvertently.
- Common examples include cloud services, productivity apps, and communication tools deployed without IT department knowledge.
- Studies suggest that 40% of IT spending occurs outside the IT department in large enterprises.

Internal vs. External Threats: Comparing Access and Impact

Security Challenge

Organizations must balance protection against external attackers while maintaining appropriate monitoring for insider threats without creating a culture of distrust.

- **Internal threats** originate from within the organization's security perimeter and exploit legitimate access.
- **External threats** come from outside the organization and must first breach perimeter defenses.
- Internal actors often have deeper knowledge of organizational systems and where valuable data resides.
- External actors typically have more resources and can target multiple organizations simultaneously.
- Detection methods differ significantly: external threats often leave evidence of intrusion while internal threats may appear as normal activity.

Following the Money: How Resource Levels Shape Attack Capabilities

- Threat actor resources directly correlate with their attack sophistication, persistence, and scale.
- **Low-resource actors** typically rely on publicly available tools and target vulnerable systems opportunistically.
- **Medium-resource actors** can develop custom tools and sustain operations over weeks or months.
- **High-resource actors** (like nation-states) can develop zero-day exploits, maintain persistent access for years, and target hardened systems.
- Resource considerations include not just financial capital but human expertise, infrastructure, and time availability.

Sophistication Spectrum: From Basic Scripts to Advanced Persistent Threats

APT Definition

An **Advanced Persistent Threat (APT)** is a sophisticated, multi-phase attack campaign conducted by well-resourced actors who maintain long-term, stealthy presence in targeted systems.

- Technical sophistication exists on a spectrum from basic automated tools to complex custom frameworks.
- Low sophistication: pre-packaged exploits, phishing kits, and DDoS-for-hire services.
- Medium sophistication: customized malware, social engineering, and lateral movement techniques.
- High sophistication: zero-day exploitation, advanced evasion, supply chain compromises, and hardware implants.
- Sophistication level influences detection difficulty, attack attribution, and required defensive measures.

Tools of the Trade: Comparing Threat Actor Arsenals

- Different threat actors employ distinctive toolsets that reflect their resources, objectives, and technical capabilities.
- Script kiddies primarily use publicly available exploits, automated scanners, and pre-packaged malware kits.
- Cybercriminal groups leverage commodity malware, phishing frameworks, and increasingly, legitimate system administration tools.
- Hacktivists favor DDoS tools, web defacement scripts, and data exfiltration utilities to maximize public impact.
- APT groups utilize custom implants, fileless malware, specialized backdoors, and sophisticated command-and-control infrastructure.

Data Theft: Who Wants Your Information and Why

Data Classification

Understanding what data different actors target helps organizations implement appropriate protections based on data classification and value.

- **Data exfiltration** involves the unauthorized transfer of data from an organization to an external location.
- Nation-states target intellectual property, defense information, and strategic intelligence to gain competitive advantages.
- Criminal groups focus on personally identifiable information (PII), payment data, and healthcare records that can be monetized.
- Hacktivists seek sensitive communications, controversial internal documents, and evidence of perceived wrongdoing.
- Insider threats often target specific high-value data based on their knowledge of where it resides and its market value.

Cyber Espionage: The Digital Spy Game

- **Cyber espionage** is the act of obtaining secrets and confidential information without permission using cyber capabilities.
- Primary practitioners include nation-states and their proxies, though corporate espionage by competitors also occurs.
- Espionage operations prioritize stealth and long-term persistence over immediate impact or monetization.
- Key targets include government agencies, defense contractors, critical infrastructure, and companies with valuable intellectual property.
- Sophisticated espionage campaigns may persist for years before discovery, with attackers adapting tactics to avoid detection.

Breaking Things: Actors Focused on Service Disruption

Impact Assessment

Service disruptions can cost organizations between $300,000 and $1 million per hour depending on the industry and systems affected.

- **Service disruption** attacks aim to prevent legitimate users from accessing systems, applications, or data.
- Common techniques include Distributed Denial of Service (DDoS), ransomware deployment, and critical system sabotage.
- Hacktivists use disruption to bring attention to causes, while nation-states may target critical infrastructure for strategic advantage.
- Criminal groups increasingly use disruption as leverage for extortion rather than as a goal itself.
- The rise of Internet of Things (IoT) has created new opportunities for massive disruption attacks.

Case Study: SolarWinds and Supply Chain Vulnerabilities

Scope

The attack affected approximately 18,000 organizations, including multiple US government agencies and Fortune 500 companies.

- In 2020, threat actors compromised SolarWinds' build system to inject malicious code into the Orion network monitoring product.
- The operation demonstrated extraordinary patience, with attackers maintaining access for months before activating backdoors.
- The US government attributed the attack to Russia's Foreign Intelligence Service (SVR).
- Victims included the US Treasury, Justice Department, and numerous technology companies.
- This case demonstrates how attacking trusted vendors can provide access to thousands of organizations simultaneously.

Extortion Economics: Ransomware and Digital Blackmail

- **Digital extortion** involves threatening to harm or expose victims unless financial demands are met.
- Ransomware encrypts critical data and demands payment for decryption keys, with average demands exceeding $200,000 in 2023.
- Double extortion attacks both encrypt data and threaten to publish stolen information if ransom isn't paid.
- Primarily conducted by criminal organizations, though some nation-states use similar tactics for financial gain.
- Organizations with time-sensitive operations (healthcare, manufacturing) or regulatory obligations are particularly vulnerable to extortion.

Show Me the Money: Financial Motivations in Cyberattacks

Evolution of Monetization

Cybercriminal business models have evolved from direct theft to sophisticated schemes including ransomware-as-a-service, cryptojacking, and business email compromise.

- **Financial gain** remains the primary motivation for most cybercriminal activity globally.
- Methods include direct theft (banking trojans), ransomware, cryptocurrency mining, payment fraud, and business email compromise.
- Criminal groups operate increasingly specialized marketplaces selling access, tools, and stolen data.
- The average cost of a data breach reached $4.35 million in 2022, creating strong financial incentives for attackers.
- Financially motivated actors typically follow return-on-investment principles, targeting the easiest victims with adequate payouts.

Hacktivism and Ideology: When Beliefs Drive Cyber Operations

- **Philosophical and political beliefs** motivate hacktivists and ideologically-driven threat actors.
- These actors view their activities as activism or civil disobedience rather than criminal behavior.
- Common targets include government agencies, corporations perceived as unethical, and organizations with opposing ideological views.
- Operations typically aim to expose perceived wrongdoing, embarrass targets, or disrupt operations to draw attention to causes.
- Unlike financial actors, ideological attackers may persist despite minimal practical success, driven by conviction rather than profit.

Ethics and "White Hat" Operations: Beneficial Breaches?

Ethical Hacking Definition

Ethical hacking involves authorized attempts to gain unauthorized access to systems, applications, or data by simulating the actions of malicious attackers.

- **Ethical motivations** in hacking include improving security, identifying vulnerabilities before malicious actors, and protecting users.
- Security researchers discover and responsibly disclose vulnerabilities through coordinated vulnerability disclosure programs.
- Penetration testers and red teams conduct authorized attacks to identify weaknesses in organizational defenses.
- Bug bounty programs provide financial incentives for ethical hackers to identify and report security issues.
- The line between ethical and unethical behavior can blur when disclosures are made without coordination or authorization.

Digital Revenge: When Personal Grudges Go Online

- **Revenge** motivates attacks by individuals with personal grievances against organizations or individuals.
- Disgruntled former employees represent a significant threat due to their insider knowledge and potentially retained access.
- Revenge-motivated attackers often focus on causing embarrassment, reputational damage, or operational disruption.
- These actors may accept greater personal risk than financially motivated attackers due to emotional investment.
- Attacks frequently include public disclosure of sensitive information, sabotage of systems, or defacement of public-facing resources.

Chaos Agents: Disruption for Disruption's Sake

Detection Challenge

Actors motivated purely by chaos often exhibit unpredictable patterns that make their behavior difficult to model and detect through conventional means.

- Some threat actors are motivated primarily by **disruption and chaos** rather than financial gain or ideological goals.
- These individuals or groups derive satisfaction from causing disorder, confusion, and system failures.
- Their targets tend to be opportunistic rather than strategic, based on vulnerability and potential for visible impact.
- Techniques range from simple website defacements to complex attacks designed to trigger cascading failures.
- Historical examples include early hacker groups like Cult of the Dead Cow and certain Anonymous operations.

Cyberwarfare: When Nations Clash in Digital Space

- **Cyberwarfare** involves state-sponsored offensive operations aimed at damaging another nation's capabilities or infrastructure.
- Unlike espionage, warfare operations prioritize impact over stealth and may target critical civilian infrastructure.
- Modern military conflicts now routinely include cyber operations alongside traditional kinetic warfare.
- Notable examples include Stuxnet (targeting Iranian nuclear facilities), attacks on Ukrainian power grid, and election interference operations.
- The absence of clear international norms and attribution challenges make cyberwarfare particularly destabilizing in international relations.

Case Studies: Notable Attacks and Their Perpetrators

Learning from History

Analyzing past attacks provides valuable insights into threat actor TTPs, motivations, and the effectiveness of various defensive measures.

- The 2020 SolarWinds supply chain attack demonstrated the sophisticated capabilities of nation-state actors (attributed to Russia).
- WannaCry ransomware in 2017 showed how criminal groups leverage stolen nation-state tools (attributed to North Korea).
- The 2014 Sony Pictures hack illustrated politically motivated destruction by state-sponsored actors (attributed to North Korea).
- The 2017 Equifax breach demonstrated how criminal organizations target and monetize massive personal data collections.
- Operation Aurora in 2009 revealed early advanced persistent threat tactics targeting intellectual property (attributed to China).

Attribution Challenges: Why Identifying Threat Actors Is Difficult

- **Attribution** is the process of determining who is responsible for a cyberattack, often with limited and ambiguous evidence.
- Sophisticated actors use false flags and borrowed techniques to mislead investigators about their identity.
- Technical evidence (IP addresses, malware code, infrastructure) can be easily manipulated or obfuscated.
- Attribution requires combining technical forensics with intelligence about known actor behaviors, capabilities, and motivations.
- Even high-confidence attributions rarely meet the standard of proof that would be required in legal proceedings.

Threat Intelligence: Practical Applications

Intelligence Lifecycle

Effective threat intelligence follows a cycle of planning, collection, processing, analysis, dissemination, and feedback to continuously improve defenses.

- **Threat intelligence** transforms raw data about threats into actionable information for security decision-making.
- Strategic intelligence helps executives understand risks and allocate resources appropriately.
- Tactical intelligence enables security teams to proactively hunt for threats based on known actor behaviors.
- Operational intelligence provides context for incident responders during active breaches.
- Intelligence sharing occurs through formal organizations (ISACs), commercial services, and informal professional networks.

Defense Strategies: Tailoring Security to Specific Threat Actors

- Understanding threat actors enables organizations to implement **threat-informed defense** rather than generic security controls.
- Defenses against nation-states require emphasis on critical data segregation, insider threat monitoring, and advanced detection capabilities.
- Protections against criminal groups focus on ransomware resilience, phishing defenses, and financial transaction safeguards.
- Mitigating insider threats requires privileged access management, behavior analytics, and data loss prevention tools.
- The MITRE ATT&CK framework maps common techniques to threat actors, enabling targeted defensive measures.

The Changing Landscape: Emerging Threat Actors and Motivations

Future Trends

The democratization of advanced attack capabilities through AI, automated exploitation tools, and attack services will continue to lower barriers to entry for sophisticated attacks.

- The line between threat actor categories continues to blur as nation-states leverage criminal proxies and criminal groups adopt nation-state techniques.
- **Artificial intelligence** is emerging both as a tool for attackers and a new category of potential threat actor if improperly secured.
- The growth of IoT and operational technology (OT) networks creates new attack surfaces and potential threat actors.
- Attacks against cloud service providers, managed service providers, and supply chains demonstrate a shift toward targeting trusted intermediaries.
- Future motivations may include manipulating markets, influencing

Putting It All Together: Comprehensive Threat Modeling

- **Threat modeling** is a structured approach to identifying potential threats, likely attack vectors, and appropriate mitigations.
- Effective models incorporate knowledge of relevant threat actors, their capabilities, and their likely motivations.
- The process begins with identifying valuable assets and mapping potential exposure to different threat actors.
- Organizations should prioritize defenses against the threat actors most likely to target their particular industry and data types.
- Regular reassessment is critical as both organizational assets and threat actor landscapes evolve.

Beyond Technology: The Human Element in Cybersecurity

Final Thought

Understanding the human motivations, behaviors, and limitations of both threat actors and defenders is ultimately more important than any technological solution.

- Technology alone cannot address the full spectrum of cybersecurity challenges posed by diverse threat actors.
- Effective security culture and awareness are essential components of defense against all threat actor types.
- Human psychology drives both attacker motivations and defender behaviors, making it central to cybersecurity strategy.
- Building resiliency requires addressing people, processes, and technology as an integrated system.
- The future of cybersecurity lies in understanding the motivations and methods of threat actors while anticipating how these will evolve.