Mapping Motivations of

Threat Actors in Cybersecurity

SanRa provides comprehensive machine learning models for modelling the psychological state, motivations and intentions of threat actors in Cybersecurity allowing practitioners to map their next moves with accuracy and precision. For corporate clients contact - corporate@sanra.co

White Paper: Motivations of Threat Actors in Cybersecurity

Introduction

In the rapidly evolving landscape of cybersecurity, understanding the motivations behind cyber threat actors is crucial for developing effective defense strategies. Cyber threat actors, ranging from individual hackers to state-sponsored groups, engage in malicious activities driven by various motivations. This white paper aims to explore the psychological and motivational factors that drive these actors, leveraging insights from psychological profiling and cybersecurity research.

Types of Threat Actors and Their Motivations

Cyber threat actors can be broadly categorized based on their primary motivations and the nature of their activities. The main categories include financially motivated actors, nation-state actors, hacktivists, cyber terrorists, thrill-seekers, and insider threats.

Financially Motivated Actors

The majority of cyber threat actors are driven by financial gain. These actors engage in activities such as distributing banking Trojans, phishing, ransomware attacks, and data theft to extort money from victims or sell stolen information on the black market. Financially motivated actors often target businesses and individuals with the aim of maximizing their monetary returns[4][5].

Nation-State Actors

Nation-state actors are typically aligned with government interests and are motivated by geopolitical objectives. These actors engage in espionage, intelligence gathering, and cyber warfare to support their nation's strategic goals. They often target critical infrastructure,

government agencies, and key industries to gain a competitive advantage or disrupt the operations of adversaries[4][5].

Hacktivists

Hacktivists are ideologically motivated individuals or groups who use hacking techniques to promote political or social causes. They target organizations or governments they perceive as unethical or harmful, aiming to disrupt their operations or expose their wrongdoings. Hacktivists are generally not financially motivated and often seek to make a statement or raise awareness about specific issues[4][5].

Cyber Terrorists

Cyber terrorists aim to cause widespread disruption and harm to achieve their ideological goals. They target critical infrastructure, businesses, and government entities to instill fear, cause economic damage, and advance their political or religious agendas. Cyber terrorism poses a significant threat due to its potential to cause large-scale damage and panic[4][5].

Thrill-Seekers

Some cyber threat actors are motivated by the thrill and challenge of hacking. These individuals, often referred to as "script kiddies," may lack advanced technical skills but use readily available tools to exploit vulnerabilities. The adrenaline rush associated with successfully breaching systems and outsmarting security measures can be highly addictive for these actors[3][5].

Insider Threats

Insider threats come from within an organization and can be particularly dangerous due to their access to internal systems and data. These actors may be disgruntled employees, contractors, or individuals with malicious intent. Insider threats can be motivated by financial gain, revenge, or ideological beliefs, and their actions can cause significant damage to an organization's operations and reputation[4][5].

Psychological Profiling of Cybercriminals

Understanding the psychological profiles of cybercriminals provides valuable insights into their motivations and behaviors. Research has identified several common personality traits and characteristics among cybercriminals, which can be mapped to different types of threat actors.

High Levels of Intelligence

Many cybercriminals exhibit above-average intelligence, enabling them to navigate complex systems and exploit vulnerabilities. This trait is particularly common among financially motivated actors and nation-state actors, who require advanced technical skills to achieve their objectives[3].

Lack of Empathy

A notable characteristic of some cybercriminals is their lack of empathy. They may not fully grasp the real-world consequences of their actions, especially when their victims are faceless entities in the digital realm. This trait is often observed in financially motivated actors and thrill-seekers[3].

Narcissism and Ego

Some cybercriminals are driven by narcissism and ego, seeking recognition and validation within the hacking community. This motivation is common among hacktivists and thrill-seekers, who take pride in their hacking skills and the notoriety they gain from their exploits[3].

Low Risk Aversion

The perceived anonymity and distance from victims in the digital world can lower the risk aversion for many cybercriminals. This factor makes it more tempting for individuals to engage in illegal activities, particularly for financially motivated actors and thrill-seekers[3].

Addictive Behavior

Engaging in cybercrime can be addictive due to the thrill of successfully breaching systems and obtaining sensitive information. This compulsive desire for more is often seen in thrill-seekers and financially motivated actors[3].

Machine Learning and Psychological Profiling

Recent research has leveraged machine learning to classify different hacker types based on the "Big Five" personality traits model (OCEAN: Openness, Conscientiousness, Extraversion, Agreeableness, and Neuroticism). This approach helps in predicting and analyzing the personality profiles of hackers, providing a nuanced understanding of their motivations and behaviors[2].

White, Black, and Gray Hats

Hackers are often categorized into White, Black, and Gray Hats based on their ethical stance and motivations:

- **White Hats**: Ethical hackers who use their skills for defensive purposes and to improve cybersecurity.

- **Black Hats**: Malicious hackers who engage in illegal activities for personal gain or to cause harm.

- **Gray Hats**: Hackers who operate in a gray area, sometimes engaging in ethical hacking and other times in malicious activities.

The machine learning model developed in the research study accurately identifies and categorizes these hacker types, providing insights into their dominant personality traits and motivations[2].

Conclusion

Understanding the motivations and psychological profiles of cyber threat actors is essential for developing targeted cybersecurity defenses. By mapping the motivations of different threat actors and leveraging psychological profiling, organizations can better anticipate and mitigate potential cyber threats. Continuous research and collaboration within the cybersecurity community are crucial for staying ahead of evolving threats and protecting critical information systems.

References

- [1] Threat Actors and their Motivations - LinkedIn

- [2] Psychological profiling of hackers via machine learning toward sustainable cybersecurity - Frontiers in Computer Science

- [3] The Psychology of Cybercriminals: Unveiling Motivations - LinkedIn

- [4] What Is a Threat Actor? - Proofpoint UK

- [5] An introduction to the cyber threat environment - Cyber.gc.ca

Sources

[1] Threat Actors and their Motivations - LinkedIn https://www.linkedin.com/pulse/threat-actors-motivations-rakesh-patra-0117c

[2] Psychological profiling of hackers via machine learning toward ... https://www.frontiersin.org/articles/10.3389/fcomp.2024.1381351/full

[3] The Psychology of Cybercriminals: Unveiling Motivations ... - LinkedIn https://www.linkedin.com/pulse/psychology-cybercriminals-unveiling-motivations-driving-sharma

[4] What Is a Threat Actor? - Definition, Types & More | Proofpoint UK https://www.proofpoint.com/uk/threat-reference/threat-actor

[5] An introduction to the cyber threat environment https://www.cyber.gc.ca/en/guidance/introduction-cyber-threat-environment

[6] What is a Threat Actor? - Types & Examples - SentinelOne https://www.sentinelone.com/cybersecurity-101/threat-actor/

[7] What is a Threat Actor? Motivations, Targeting and Staying Ahead https://www.criticalstart.com/what-is-a-threat-actor-motivations-targeting-and-staying-ahead/

[8] The Psychology of Cybercriminals: Understanding the Mind of a ... https://www.linkedin.com/pulse/psychology-cybercriminals-understanding-mind-hacker-sharma

[9] [PDF] Psychological profiling of hackers via machine learning ... - Frontiers https://www.frontiersin.org/articles/10.3389/fcomp.2024.1381351/pdf?isPublishedV2=False

[10] The Psychology of Hackers - LinkedIn https://www.linkedin.com/pulse/psychology-hackers-dale-gibler

[11] What is a Threat Actor? - IBM https://www.ibm.com/topics/threat-actor

[12] How Are Cybercrime and Psychology Related? https://online.nsu.edu/degrees/technology/master-of-science-cyberpsychology/cybercrime-and-psychology-related/

[13] What is a Cyber Threat Actor? - CrowdStrike.com https://www.crowdstrike.com/cybersecurity-101/threat-actor/

[14] The Motivation of Cyber Threat Actors: Who's after your stuff? https://stratixsystems.com/the-motivation-of-cyber-threat-actors-whos-after-your-stuff/

[15] Is there a cybercriminal personality? Comparing cyber offenders and ... https://www.sciencedirect.com/science/article/pii/S074756322200396X

[16] 4 What are the motivations for cybercrime? | OpenLearn https://www.open.edu/openlearn/health-sports-psychology/psychology/the-psychology-cybercrime/content-section-4

[17] [PDF] 1 Psychology of cybercrime - Assets - Cambridge University Press https://assets.cambridge.org/97811070/04443/excerpt/9781107004443_excerpt.pdf

[18] Personality Characteristics - Catb.org http://www.catb.org/esr/jargon/html/personality.html

[19] The Psychology of Cybercriminals: Understanding Motivations and ... https://moldstud.com/articles/p-the-psychology-of-cybercriminals-understanding-motivations-and-behavior

[20] The psychological profile of a hacker with emphasis on security ... https://www.infosecinstitute.com/resources/security-awareness/the-psychological-profile-of-a-hacker-with-emphasis-on-security-awareness/