Inside the Mind of the Adversary: Unmasking Credential Access Attacks — A Four-Part Deep Dive Series

In today's identity-driven threat landscape attackers no longer need to break in when they can simply log in. Credential access attacks have become the cornerstone of modern cyber intrusions, powering everything from ransomware deployments to supply chain compromises. As identity becomes the new perimeter, understanding how, when, and why credentials are targeted is critical to defending your enterprise.

To help organizations strengthen their defenses, our Cyber Threat Intelligence team is launching a four-part investigative series dedicated to exposing how adversaries steal, abuse, and weaponize credentials and how defenders can stop them.

Part 1: Credential Access Attack Overview, Methods, Motivations, and CISO Insights
The first article lays the groundwork by defining credential access attacks and explaining why they remain one of the most exploited techniques. It explores how adversaries obtain, use, and conceal stolen credentials while examining the broader business implications of identity compromise. Readers will gain a clear understanding of the most common attack methods, including password spraying, brute force attempts, credential gathering, and leaked credentials.

Part 2: Mapping the Adversary, Targeted Industries, Threat Actors, and TTPs
The second article shifts the focus from foundational knowledge to actionable intelligence. It identifies the industries most frequently targeted by credential access campaigns and highlights the key threat actors driving these operations. The discussion includes a detailed look at the MITRE ATT&CK techniques most often employed, along with a timeline analysis that tracks attack activity across months, days, and even hours. By mapping adversary behaviors and operational rhythms, readers will gain valuable context for anticipating and disrupting attacks before they escalate.

Part 3: Inside the Cyber Range, Simulating a Credential Access Attack
The third article brings theory into practice through a detailed cyber range breakout that demonstrates how a credential access attack unfolds from start to finish. Readers will gain insight into each stage of the operation, including the commands executed, the logs generated, and the artifacts left behind. This breakout illustrates the warning signs that indicate credential compromise and provides defenders with a framework for detecting and containing an attack before it results in lateral movement or data loss.

Part 4: Attack Teardown, Logging, Detection, and Mitigation Strategies
The final article dissects a complete credential access attack chain to show how adversaries operate at each stage of the intrusion. It examines key log sources, forensic indicators, and system telemetry that reveal attacker movement, translating these technical findings into practical detection and mitigation strategies. This series concludes with a comprehensive set of recommendations on identity hardening, continuous monitoring, and long-term credential protection, enabling organizations to build sustainable resilience against future credential-based threats.

Why This Series Matters

Credentials are the currency of compromise and the keys that unlock an organization’s most valuable assets. Every stolen password, token, or API key can open the door to unauthorized access, lateral movement, and data theft. This series reveals the complete credential access attack lifecycle, from the first signs of compromise through post-incident response, giving security teams the knowledge and tools to detect, disrupt, and stop adversaries before damage occurs.

Stay tuned for Part 1, “Credential Access Attacks: Methods, Motivations, and the CISO Overview,” launching this week. Join us as we expose the hidden economy of stolen credentials and show how organizations can transform identity from a point of vulnerability into a powerful line of defense.