ANOMALI

GUIDE

Use Case: Mitigating Compromised Credentials with the MITRE ATT&CK® Framework

2025 Strategies to Mitigate Attacks that Use Compromised Credentials with the MITRE ATT&CK® Framework

Compromised credentials — valid credentials, such as usernames and passwords, that have been captured by an adversary — are the most widespread threat facing organizations today. Attacks using compromised credentials pose a particular challenge for security teams since these attacks allow cybercriminals to access sensitive systems and data in the guise of a legitimate user, undetectable by standard security measures, such as antivirus and anti-malware software.

Compromised Credentials' High Price Tag

While IBM and the Ponemon Institute report that the average cost of a data breach in the U.S. is approaching $10 million per incident, recent high-profile breaches using compromised credentials show that their impact far exceeds financial losses.

- **Colonial Pipeline (2021):** In one of the most notorious breaches of recent years, attackers used a compromised VPN password to steal nearly 100 GB of data and deploy ransomware. The company had to shut down its 5,500-mile pipeline, triggering widespread fuel shortages and price spikes. It also paid a $5 million ransom and suffered significant operational and reputational damage.
- **Okta (2024):** As a leader in identity and access management (IAM), Okta was particularly embarrassed by a significant data breach using the credentials an employee had saved to their personal Google account. The breach affected high-profile Okta customers, including Cloudflare and BeyondTrust, amplifying the reputational damage.
- **Norton (2023):** Attackers used previously leaked credentials from the dark web to breach this longtime cybersecurity mainstay. Over 925,000 customers were affected — including some who had saved their passwords in the company's password manager.
- **23andMe (2023):** In an attack targeting some of the most sensitive personal data, attackers used compromised credentials to access 14,000 user accounts, then used their stored genetic and family tree information to expose the data of another 6.9 million individuals. The company faced extensive criticism and agreed to a $30 million settlement.

The good news is that there is a way to understand and develop strategies to address these types of vulnerabilities with the MITRE ATT&CK framework.

What is the MITRE ATT&CK framework?

MITRE ATT&CK is a globally accepted foundation and knowledge base for any person or organization to use to improve security. ATT&CK stands for Adversarial Tactics, Techniques & Common Knowledge. It is a comprehensive and evolving list of tactics and techniques that highlights different ways that attackers can infiltrate networks or systems.

The framework provides organizations with the ability to better fight adversaries through:

- Information about all the adversarial techniques
- Details of threat groups that have utilized these techniques
- How to detect and mitigate tactics and techniques

Tactics describe what the attacker is trying to do at a given phase of the attack while techniques describe the various technical ways attackers have successfully infiltrated organizations.

How Compromised Credentials Escape Detection

With all these techniques at adversaries' disposal, compromised credentials attacks are exceptionally difficult for security analysts to counter.

- **Legitimate appearance:** Compromised credentials allow attackers to impersonate authorized users, making their activities appear legitimate to traditional security tools. As a result, attackers can often operate undetected within networks for extended periods, escalating privileges and moving laterally without raising suspicion.
- **Evolving attack techniques:** Adversaries are constantly developing new methods to acquire and exploit credentials, such as more sophisticated phishing, social engineering, and multifactor authentication (MFA) fatigue attacks in which attackers undermine multi-factor authentication by repeatedly sending MFA requests to a victim's email, phone, or other registered devices.
- **Data volume and complexity:** The sheer volume of authentication events and user activities in modern networks makes it difficult to identify subtle indicators of compromised credentials. Security teams struggle to differentiate genuine threats from false positives in vast amounts of log data and alerts across complex enterprise environments.

MITRE ATT&CK Enterprise Tactics

There are 14 different tactics that represent the different stages of a cyberattack. Compromised credentials falls under the MITRE ATT&CK category TA0006: Credential Access.

ID	Tactic	Description
TA0003	Reconnaissance	Gathers information they can use to plan future operations
TA0042	Resource Development	Establishes resources they can use to support operations
TA0001	Initial Access	Tries to get into the network
TA0002	Execution	Tries to run malicious code
TA0003	Persistence	Tries to maintain their foothold
TA0004	Privilege Escalation	Tries to gain higher-level permissions
TA0005	Defense Evasion	Tries to avoid being detected
TA0006	Credential Access	Tries to steal account names and passwords
TA0007	Discovery	Tries to figure out an environment
TA0008	Lateral Movement	Tries to move through your environment
TA0009	Collection	Tries to gather data of interest for their goal
TA0011	Command and Control	Tries to communicate with compromised systems to control them
TA0010	Exfiltration	Tries to steal data
TA0040	Impact	Tries to manipulate, interrupt, or destroy your systems and data

The ATT&CK framework outlines numerous techniques within TA0006: Credential Access.

ID	Tactic	Description
T1110	Brute Force	• A trial-and-error method that systematically guesses the password using a repetitive or iterative tool until the correct one is found • Relies on computing power
T1557	Adversary-in-the-Middle	• Sets up a server that sits between the target and the real site • Redirects the user to the server instead of the real site • Intercepts and modifies the information being exchanged
T1555	Credentials from Password Stores	• Searches for common password storage locations to obtain user credentials
T1212	Exploitation of Credential Access	• Takes advantage of a programming error in a program, service, or within the operating system to execute code
T1187	Forced Authentication	• Ex: Sends an attachment to a user through spearfishing that contains a resource link or a specially crafted file • Once document is opened or link is clicked, attempts authentication and sends information, including the user's hashed credentials, over SMB to the adversary-controlled server
T1606	Forge Web Credentials	• Forge credential materials that can be utilized to gain access to applications or internet services • Differs from other behaviors — the credentials are new and forged by the adversary instead of stolen
T1056	Input Capture	• Utilizes methods to capture user input to obtain credentials or collect information either through transparent means or by deceiving the user into providing information into what they believe is a genuine service
T1556	Modify Authentication Process	• Modifies authentication processes and mechanisms to access user credentials or enable unwarranted access to accounts. • By modifying the process, the adversary can authenticate a service or system without a valid account
T1111	Multi-Factor Authentication (MFA) Interception	• Targets MFA to gain access to credentials • Techniques can be utilized to intercept and bypass MFA
T1621	Multi-Factor Authentication (MFA) Request Generation	• Generates MFA requests sent to users such as abusing the automatic generation of push notifications to MFA services such as Duo Push, Microsoft Authenticator, Okta, or similar
T1040	Network Sniffing	• Uses the network interface on a system to monitor or capture information sent over a wired or wireless connection • Passively sniffs network traffic to gain access to data or uses span ports to capture larger amounts of data
T1003	OS Credential Dumping	• Dumps credentials to obtain login and credential material, normally in the form of hash or clear text password
TA0040	Impact	• Tries to manipulate, interrupt, or destroy your systems and data
T1528	Steal Application Access Token	• Steals application tokens as a means of acquiring access to remote systems and resources • By stealing account API tokens in cloud and containerized environments, adversaries may be able to access data and perform actions with the permissions of these accounts
T1649	Steal or Forge Authentication Certificates	• Digital certificates are often used to sign and encrypt messages and/or files or certificates are used as authentication material • Steals or forges these certificates used for authentication to access remote systems or resources
T1558	Steal or Forge Kerberos Tickets	• Kerberos is an authentication protocol widely used in modern Windows domain environments • Subverts Kerberos authentication by stealing or forging Kerberos tickets without having access to an account's password
T1539	Steal Web Session Cookie	• Web applications and services often use session cookies as an authentication token after a user has authenticated to a website; cookies are often valid for an extended period, even if the web application is not actively used • Steals web application or service session cookies and uses them to gain access as an authenticated user without needing credentials
T1552	Unsecured Credentials	• Credentials can be stored and/or misplaced in many locations on a system • Searches compromised systems to find and obtain insecurely stored credentials

Indicators of User Credential Compromise

Adversaries will try every tool in their arsenal to avoid detection. It's imperative that organizations and users continually monitor systems to detect when an account has been compromised. Indicators of a compromised account may include:

- **Unusual outbound traffic:** Network activity in which a significant amount of data is being sent from a system or network that deviates from its typical usage patterns
- **Unusual login locations and times:** Login attempts to accounts from a location or at a time that is significantly different from where a user typically logins
- **Impossible travel:** Logins from two different locations in a suspicious amount of time
- **Multiple failed logins:** Multiple consecutive login failures from the same account within a short time
- **Irregular access to sensitive data:** Unauthorized or unusual access to confidential information without proper permission
- **Suspicious configuration changes:** Unexpected or unauthorized changes made to system settings

Strategies in 2025 to Detect Compromised Credentials

Organizations may not be able to completely prevent credentials from being misused — it only takes one slip for a valid login to fall into the wrong hands — but you can mitigate the resulting risk by implementing the strategies below:

- **Enable MFA:** Also known as two-step authentication, MFA requires users to provide more than one form of identification to log in to an account. While passwords protect digital assets, MFA acts as an additional layer of security to prevent unauthorized users from accessing these accounts, even when a password has been stolen.
- **Profile your adversaries:** Understand the enemy and their tactics by identifying their motivations and capabilities that may be specific to your organization. By profiling your adversaries, you can find similarities among them that help adapt defenses against emerging threats, prioritize resources, and take proactive action. ATT&CK continually updates the tactics and techniques of existing and new adversaries to provide organizations with real-time knowledge of their attackers.
- **Implement user entity and behavior analytics (UEBA) capabilities:** UEBA collects information from various systems, applications, networks, and devices to establish baseline behavior patterns. Using machine learning and advanced analytics, UEBA identifies abnormal behavior patterns to help identify sophisticated cyberattacks. UEBA helps organizations detect techniques for compromised credentials outlined in ATT&CK more quickly than rules-based detections.
- **Continuously monitor the attack surface:** Actively monitor digital assets for potential vulnerabilities like outdated software, misconfigurations, or exposed sensitive data on an ongoing basis to help identify new threats and points of exploitation. Mapping vulnerabilities to ATT&CK helps defenders chart their operational controls to see where they have weaknesses against certain actors.
- **Accelerate threat hunting:** Actively seek out malicious activity by using a combination of human expertise and advanced analytics to analyze logs and data instead of merely reacting to alerts. Analysts can proactively identify hidden threats that have already evaded traditional security mechanisms and have already found a presence in an organization's network.
- **Elevate intelligence:** ATT&CK provides details on nearly 70 threat actors and groups and the techniques and tactics they use to gain access to an organization's network. Leverage threat intelligence feeds to identify potential indicators of compromise (IoCs), such as compromised credentials, before attacks occur. This proactive approach helps detect threats in your environment by tracking ATT&CK techniques, tactics, and procedures (TTPs), as well as threat actors, campaigns, security bulletins, and vulnerabilities.

Detecting Compromised Credentials with the Anomali Security and IT Operations Platform

Understanding the MITRE ATT&CK framework helps organizations understand adversaries' underlying tactics, techniques, and procedures (TTPs). The right tools, like those provided by Anomali, utilize evidence-based knowledge to help organizations put that understanding into action.

Anomali's Security and IT Operations Platform leverages a deep understanding and integration of the MITRE ATT&CK framework along with the largest curated access to threat intelligence to detect anomalous behavior. It orchestrates a fast and effective response, ensuring that even fully authenticated threat actors cannot succeed in their attempts to harm your systems, data, and business.

Anomali: The Future of SIEM

Anomali is a groundbreaking AI-Powered Security and IT Operations Platform that provides comprehensive visibility, speed, AI, and world-class threat intelligence in one easy-to-use integrated platform. Only Anomali combines ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR, and TIP to consolidate your tech stack and empower your team to do more with less.

Innovative, Effective Technology

Cybersecurity solutions for organizations of all sizes. AI-Powered intelligence-driven solutions for a more secure world. That's Anomali.

Discover how Anomali can help you prevent compromised credential attacks in your organization — schedule a demo.

Security and IT Operations Done Differently.

Anomali is the leading AI-Powered Security and IT Operations Platform that delivers mind-blowing speed, scale, and performance at a fraction of the cost. Our cloud-native approach modernizes the delivery of legacy systems, combining ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR and TIP to deliver security analytics that enable our customers to detect, investigate, respond, and remediate threats in one integrated platform.

Request a demo to learn more about the Anomali AI-Powered Security and IT Operations Platform.

ANOMALI