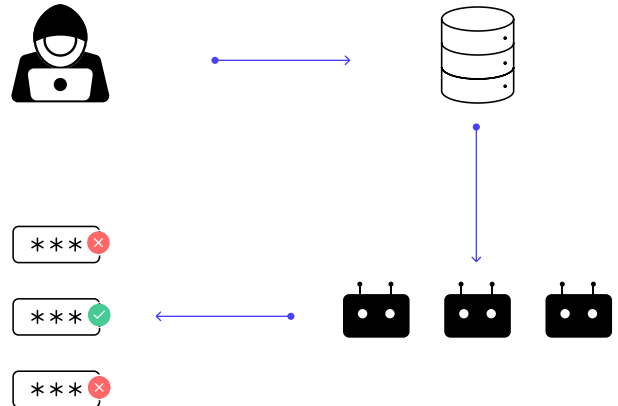


Credential Stuffing Detection

Strengthening Your Cyber Defenses Against Invasive Attacks

The Growing Threat of Credential Stuffing

Credential stuffing represents a significant cybersecurity challenge, where attackers access accounts across services using stolen credentials. It differs from brute force attacks by using advanced automation, like bots, to try stolen passwords on numerous accounts. Its covert nature makes it especially dangerous, enabling attackers to remain undetected and cause significant damage. Credential stuffing can lead businesses to face financial losses, privacy breaches from exposed personal data, and significant reputation harm, potentially causing customer and business loss.



Alarming Statistics in Password Security

The password habits of internet users, which reveal concerning trends, emphasize the urgent need for enhanced security measures and greater awareness to address the escalating risk of credential stuffing attacks.

- "123456" continues to be the most common password choice, indicating a lack of password complexity.
- Nearly two-thirds of Americans are found to reuse passwords across multiple accounts, creating a massive security vulnerability.
- A disturbing 13% of users go to the extent of using the exact same password for every online account they have.

Why Traditional Security Measures Fall Short

Traditional security controls are often inadequate in the face of sophisticated credential stuffing attacks. Attackers can bypass these measures using distributed botnets or by strategically prolonging the attack timeline, leading to significant gaps in security defenses. This highlights the need for a more advanced and comprehensive approach to cybersecurity.

The screenshot shows the Wallarm dashboard for Credential Stuffing Detection. It displays 21 attacks and 191 credentials detected in the last 7 days. The system is enabled. It lists recommended authentication endpoints for login, with password and login location patterns. A reaction to credential stuffing is also shown, with 4.5M of 10M (45%) of compromised user accounts.

Innovative Detection and Monitoring

Wallarm's advanced detection system is designed to combat the sophisticated nature of credential stuffing attacks. By focusing on authentication endpoints, a key area of vulnerability, Wallarm's system tracks and analyzes each login attempt. This meticulous approach allows for the accurate identification of compromised credentials being used, providing an essential layer of security.

Distinctive Benefits of Wallarm's Credential Stuffing Detection versus Conventional Tools



Exceptional Accuracy in Detection

Wallarm distinguishes itself through solutions that deliver high levels of accuracy in detection. These solutions target authentication endpoints, essential areas of vulnerability, ensuring superior accuracy in the identification and thorough analysis of every API-based login attempt. Contrasting with the broader approach of generic alternatives, Wallarm specifically concentrates on authentication endpoints, which are critical points of vulnerability.



Customization Powered by Intelligence

Wallarm's platform is distinguished by its intelligence-driven customization. It enables specific adjustments and configurations, ensuring a response tailored to your unique needs. This approach guarantees a more accurate alignment with security policies compared to standard, broad-spectrum solutions.



Automated Security and Privacy Measures

Wallarm's strategy in combating credential stuffing includes sophisticated automated systems. These systems not only secure your business operations, but also safeguard your reputation against such intricate threats. The automation efficiently counters attacks while preserving the confidentiality of sensitive data.

Wallarm Credential Stuffing Detection: Multifaceted Detection and Comprehensive Protection

Wallarm's approach to combating credential stuffing includes multiple detection methods. It combines the identification of brute force attempts with behavioral analysis through API Abuse Prevention. The newly added credential stuffing detection feature grants security analysts enhanced control, allowing for the identification of each instance where a known-compromised credential is used.

Supported by a vast database of compromised passwords, Wallarm enables organizations to quickly detect compromised user accounts. This feature provides more robust protection against credential stuffing threats.

The Credential Stuffing Detection capability is available as part of Wallarm's Advanced API Security platform and is integrated into the latest version of the Wallarm node. For more detailed information about this feature, users are encouraged to consult our documentation below.

Further Resources & Support

To gain further insight into protecting against credential stuffing, Wallarm provides a wealth of resources. Explore our comprehensive guide in the Learning Center. Alternatively, schedule a demo with Wallarm to discover how we safeguard against such attacks or find out more from our corporate blog or our information on Wallarm's Credential Stuffing Detection webpage.