Stopping Credential Misuse and Attacks

Prevent attacks and data theft by detecting and stopping the use of leaked credentials.

KEY BENEFITS

Prevent credential-based attacks
Real-time, automated checks against one of the industry's most comprehensive databases of leaked, stolen, and breached credentials.

Leverage automation
Automate leaked credential policy configuration and enforcement via command-line interface (CLI) APIs.

Flexibly mitigate risk
Take fast, decisive, and flexible actions against login attempts that use breached or fraudulent credentials.

Ensure complete security
Credential checks use a salted hash of the credentials, not cleartext.

Initiate and control responses
Response options to leaked or stolen login credentials that are appropriate for your business.

Why Credentials Pose a Top Security Risk

It's a fact of today's digital life: With users needing to log in to so many different applications, websites, and other software and online entities, credential reuse is almost inevitable. Unfortunately, many users re-use the same credentials across their personal and business accounts.

So, when a social network or other consumer-facing application or website is hacked and credentials are harvested, the leaked credentials provide a great way for attackers to launch account takeover (ATO) attacks on or steal critical personal data from users' accounts. It also makes it easy for attackers to use those same compromised credentials on unsuspecting users' business accounts. It's no surprise that phishing attacks targeting credentials are constantly on the rise, too.

Many businesses experience an alarming rate of credential stuffing attacks. Cybercriminals use automation tools, bots, botnets, and compromised credentials from personal and business accounts to obtain personally identifiable information (PII), protected health information (PHI), or other sensitive personal data. Then they either sell this info on the dark web to be used for social engineering as part of a larger ransomware attack or other attack type.

According to F5 Labs, approximately 3 billion credentials are stolen in a year. A recent report from F5 Labs called out credential stuffing as a top security threat. A breach leveraging compromised user credentials can significantly impact the user or their business, based on the type of account under attack (for example, bank account, health insurance ID, corporate applications, and so on). Protecting against the fraudulent use of credentials on public-facing or internal corporate websites and applications continues to be a challenge for organizations.

WHEN A SOCIAL NETWORK OR OTHER CONSUMER-FACING APPLICATION OR WEBSITE IS HACKED AND CREDENTIALS ARE HARVESTED, THE LEAKED CREDENTIALS PROVIDE A GREAT WAY FOR ATTACKERS TO LAUNCH ACCOUNT TAKEOVER (ATO) ATTACKS ON OR STEAL CRITICAL PERSONAL DATA FROM USERS' ACCOUNTS.

Addressing Leaked Credentials–A Modern Approach

For today's SecOps teams, a modern approach to dealing with leaked credentials has to include:

- Preventing compromised credentials from being used to access applications by accurately detecting and mitigating their use.
- Making sure leaked, compromised credentials are automatically detected, assessed, and rejected.
- Improving risk response efficacy and proactively enhancing their organization's security posture.

KEY FEATURES

Accurately detects and prevents attacks
Intelligent, automated, and accurate leaked, breached, and fraudulent credential detection in real-time.

Automatically updates breached credentials
Provides automated updates from one of the most powerful, comprehensive leaked credential databases as new leaked or stolen credentials and data become available.

Enterprise-grade, bespoke mitigation
The enterprise or application owner can manage and enforce policies and responses to detected leaked or stolen credentials.

F5 Leaked Credential Check can help. It's an add-on threat intelligence subscription for F5 Advanced Web Application Firewall (AdvWAF). Leaked Credential Check stops leaked or stolen credentials from being used to access personal or business applications. It automatically detects and mitigates compromised credential use. If compromised credentials are detected during an attempted login, Leaked Credential Check enables several mitigation options for SecOps teams to enact, individually or collectively, including:

- Requiring the user to employ multi-factor authentication (MFA) before granting access.
- Redirecting the user to another application page; for example, a customer support web page.
- Responding to the suspicious login with a preset page requesting further action by the user, such as contacting customer support.
- Blocking the user and their login from accessing the application.
- Sending an alert to the SecOps team to take additional action.

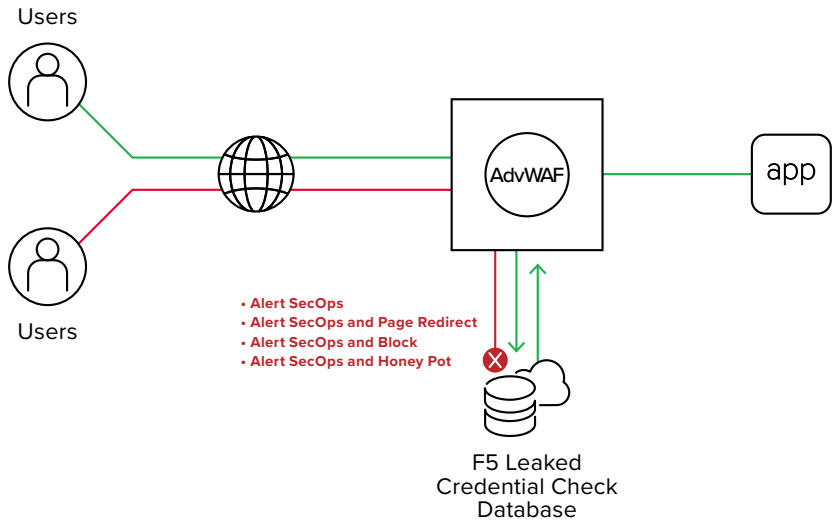

Figure 1: F5 Leaked Credential Check screens users based on a comprehensive leaked-credential database, triggering real-time mitigations.

F5 LEAKED CREDENTIAL CHECK USES A MODERN APPROACH TO SAFEGUARD ORGANIZATIONS AGAINST MALICIOUS AUTOMATED CREDENTIAL ATTACKS. WHAT SETS IT APART IS ITS ADVANCED ANALYTICS, DEVELOPED BY F5 LABS AND SHAPE SECURITY.

Why F5 Leaked Credential Check?

F5 Leaked Credential Check uses a modern approach to safeguard organizations against malicious automated credential attacks. What sets it apart is its advanced analytics, developed by F5 Labs and Shape Security. Leaked Credential Check is easy to deploy; it's an add-on feature for F5 Advanced WAF and available as a subscription-based service that can be enabled in minutes.

Built on the efficacy of Shape Enterprise Defense and the research strength of F5 Labs, Leaked Credential Check provides enterprises with a real-time focus on and visibility into attacks that use leaked and stolen credentials. It empowers enterprises to identify and stop even the most powerful, sophisticated credential-based attacks. F5 Leaked Credential Check also proactively identifies vulnerable credentials of customers and employees, delivering preemptive credential defense.

To learn more, visit f5.com/products/security/advanced-waf or contact an F5 representative.