THINK APP SECURITY FIRST

CREDENTIAL STUFFING
A SECURITY EPIDEMIC

USERNAME/PASSWORD

USERNAME/PASSWORD

USERNAME/PASSWORD

USERNAME/PASSWORD
INTRODUCTION

The world set a new record for data breaches in 2016, with more than 4.2 billion\(^1\) exposed records, shattering the former record of 1.1 billion in 2013. But if 2016 was bad, 2017 is shaping up to be even worse. In the first six months of 2017, there were 2,227 breaches reported, exposing over 6 billion records and putting untold numbers of accounts at risk.\(^2\)

Out of all these stolen records, a large majority include usernames and passwords, which are leveraged in 81 percent of hacking-related breaches according to the 2017 Verizon Data Breach Investigations Report.\(^3\)

Faced with ever-growing concerns over application and data integrity, organizations must prioritize identity protection in their security strategies. In fact, safeguarding the identity of users and managing the level of access they have to critical business applications could be the biggest security challenge organizations face in 2017.

\(^1\) https://pages.riskbasedsecurity.com/hubfs/Reports/2016%20Year%20End%20Data%20Breach%20QuickView%20Report.pdf


\(^3\) http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
In a credential stuffing attack, cybercriminals turn to the dark web to purchase previously stolen usernames and passwords. They then make repeated attempts with automated tools to “stuff” the login fields of other websites with the credentials to gain access to accounts held by corporate users or customers. When a “stuffing” attempt is successful, the attacker uses the account for fraudulent purposes. There’s typically a 1 to 2 percent success rate, which means that if a cybercriminal purchases 1 million stolen credential records (for sale on the dark web for fractions of a cent each⁴), they can generally gain access to 10,000 to 20,000 accounts.

NEARLY 17% OF PEOPLE WERE STILL SAFEGUARDING THEIR ACCOUNTS WITH THE PASSWORD “123456” IN 2016.

These attacks wouldn’t be successful if people used different usernames and passwords for each site or application they access. Instead of taking the time and energy to craft unique credentials for each of their many accounts, nearly three out of four users reuse and recycle credentials across accounts.⁵

The reality is that no matter how strong your organizational security is, if your users or customers reuse their passwords—and they probably do—then the likelihood is that their credentials have already been stolen. With the explosive rise of credential theft and the relative ease with which cybercriminals can use automated tools to gain control of user accounts, organizations are justifiably concerned about the security of their applications and data.

The question is: how can you prevent, or at least mitigate, these attacks?

⁵ https://www.entrepreneur.com/article/246902
A GUIDE TO STOPPING CREDENTIAL THEFT

Let’s start with the bad news: there’s no simple switch you can flip that will protect your organization from credential stuffing attacks. However, there are a number of steps you can take to drastically reduce the likelihood of being a victim of a successful attack. Train your users to implement more secure password practices, while working on the corporate side to shore up your own security.

PEOPLE AND POLICIES: TRAIN, REPORT, ENHANCE

Besides obtaining and leveraging previously stolen credentials, phishing is the next best way for cybercriminals to steal credentials to be used for credential stuffing. You can help boost awareness about phishing among your employees by offering training and education. While this will not completely eliminate the chance of a successful phishing attack, a solid understanding of the way that cybercriminals work can help users better protect themselves, and the organization. Start with training your users to spot phishing attacks. You can devise your own tests, or use a free online test. You can further empower users with some password management best practices. The most significant takeaway for your employees is that no one should ever use network login credentials on any third-party site, because if that site is compromised, then cybercriminals will have access to your corporate network and any applications within. If you learn that employees have used their corporate credentials on other sites, ensure that they change them immediately.

It’s also a good idea to assume that some percentage of your users do reuse passwords, and to force a reset of all users’ passwords following a high-profile breach, like the Yahoo! or LinkedIn breaches.

Keep in mind that no matter how much training you provide, people are human and credential theft is still a possibility. Set up policies that make it easy for users to report an incident to IT immediately if they think they’ve clicked on a malware link in a phishing email or have mistakenly divulged their credentials. If IT gets the report quickly, a security administrator can help clean the system, reset passwords, alert other employees of the scam, and, most importantly, adjust your corporate security controls so other users don’t get taken in by the same attack.

8 http://resources.infosecinstitute.com/top-9-free-phishing-simulators/
CREDENTIAL STUFFING: AN SECURITY EPIDEMIC

When architecting your application security strategy to defend against credential stuffing attacks, you may have to address two different types of user. A corporate employee will embrace—or at least follow—more burdensome processes like multifactor authentication (MFA). However, an ecommerce or retail customer has much less tolerance for anything that complicates the login process. There are steps you can take to protect both committed employees and more casual users.

Secure and encrypt

A robust web application firewall (WAF) is the first piece of your armor against credential stuffing attacks. A full-featured modern WAF can provide advanced bot detection and prevention, which is key because most attacks are launched using automated programs. By analyzing behavior, such as IP location, time of day, and connection attempts per second, a WAF can help your security team identify non-browser login attempts. Additionally, using signature matching, your WAF makes it easy to whitelist desirable bots (such as search engine bots) and allow them access to your site.

A WAF can also help you detect whether stolen information is being used in a login attempt by running usernames and passwords against a known list of compromised credentials. In addition, your WAF allows your security team to monitor potential credential stuffing attacks by tracking multiple failed login attempts over a given amount of time. For proactive defense, set your WAF to prevent more than x login attempts per x seconds, which can slow down an incoming attack and give you time to adjust your security settings.

Another step you can take to reduce your attack surface is to use geo-intelligence to filter connections from known bad IP addresses or geographical regions. And once you’ve identified an attacker, it’s a good idea to add bad IP addresses and device fingerprints to a threat feed and integrate that with other security solutions that may need to block or detect that activity. Keep in mind that this may be a very temporary fix since many bot operators interchange IP addresses frequently.

TECHNOLOGY: DIFFERENT USE CASES, DIFFERENT DEFENSES

WAF PROTECTION

A full-featured modern WAF can provide advanced bot detection and prevention, which is key because most attacks are launched using automated programs.
Dynamic form obfuscation can make your site's login form much more difficult for an attacker to discover. Instead of naming the input fields with identifiable labels, such as “passwd” or “usrnme,” dynamic field obfuscation changes the field names into long strings of obscure characters that change frequently, making it impossible for the attacker's bot to recognize the correct fields and insert the stolen credentials.

Finally, you can also ensure that data in the browser or your mobile applications is encrypted to protect all the information transferred from users and render any intercepted data worthless. As an added layer of security, you can force the form parameters to be encrypted using a client-side function. Automated credential stuffing tools will be hard-pressed to properly execute the page to encrypt the form fields and send the correct secure channel cookie. When the bots submit unencrypted credentials, it will trigger a system alert to let your security team know that a credential stuffing attack may be taking place.

**Take control of authorization**

While a WAF can help defend against credential stuffing attacks, you can vastly reduce the application's attack surface by implementing token-based authorization, also known as OAuth (Open Authorization). This enables users to access an application without having to provide their credentials to that application itself. Once the user establishes identity by authenticating to a site like Facebook, Google, Microsoft Azure, or even your own authorization server, a one-time short-lived access token is issued to the application the user is connecting to. The application does not require additional credentials, which makes it convenient for the user. In addition, the trusted source, or “authorization server,” ensures secure authentication and drastically reduces the effectiveness of credential stuffing attacks.

Token-based authorization is also a great solution for protecting your APIs from credential stuffing attacks. APIs are a prime target for these attacks because they're already designed to be accessed programmatically (software to software), making separating authorization out onto an OAuth server even more critical. Access to an API via OAuth frees application developers from hard-coding login credentials into the application, thus increasing API security. Another benefit is that tokens can be configured to provide varying degrees of access rather than only full access or no access.

Most organizations have several applications, each with its own user login or API. And because OAuth itself is not natively secure, you run the risk of it being implemented in a vulnerable manner.

Fortunately, you can decrease risk by managing access to applications, network resources, and APIs, all from one place: a centralized access gateway that can translate OAuth authorization back to the application. This gives you a single point of control.
CREDENTIAL STUFFING: AN SECURITY EPIDEMIC

Mutli Factor Authentication

To prevent a credential stuffing attack, a user is challenged to provide more than their static password to prove identity.

For all access decisions, mitigates your risk of an insecure OAuth implementation, and saves precious engineering time spent building in the authorization framework.

There are other security benefits to implementing a secure access gateway, especially for corporate employees. When you funnel all authentication and access requests through one high-performance gateway, you can offer your users a consistent experience that lessens the chances that they’ll fall for phishing attempts. With this gateway also come single sign-on and risk-based MFA, which are key pieces of an identity security solution. While all authentication and access requests go through the centralized access gateway, not all requests are equal. Authentication challenges and access decisions may differ based on a number of risk factors, including the user’s role, device, geographical location, and time of day, as well as the sensitivity of data within the application. If a profile returns several high-risk factors, the gateway can prompt the user for a second or even third factor to verify their identity before granting access. When a user is challenged to provide more than just a static password to prove identity, credential stuffing attacks are unsuccessful.

Attackers steal millions of credentials or buy them on the Dark Web.

Automated bots make repeated attempts to "stuff" application login forms with the stolen credentials.

An additional token is required, and the attack is unsuccessful.

Healthcare data

Credit card data

Financial data

Passport data

Intellectual property
IDENTITY SECURITY = ORGANIZATIONAL SECURITY

As identities become the prime targets of cybercriminals, organizations must understand that identity and access security is the key to ensuring the integrity of your applications and data. By combining user training, strong and consistent corporate policies, a robust web application firewall, and a centralized authentication and authorization gateway, organizations can prevent, or at least mitigate, today’s increasingly powerful and persistent credential stuffing attacks.

For more information about application protection, visit f5.com/security.
Always-on, always-connected apps can help power and transform your business—but they can also act as gateways to data beyond the protections of your firewalls. With most attacks happening at the app level, protecting the capabilities that drive your business means protecting the apps that make them happen.