Auth0

Credential stuffing attacks: What they are and how to combat them

Credential stuffing attacks:

What are they and how to combat them

Compromised user credentials are a common attack vector, and can lead to sustained, costly attacks. As an Identity-as-a-service provider (IDaaS), Auth0 sees a large number of attacks targeting user credentials across our customer base. Some of our customers are under attack nearly 24/7.

Known as credential stuffing attacks, these attempts to compromise user accounts with stolen credentials are a difficult problem to solve. More than 80 percent of companies state it is difficult to detect, fix, or remediate credential stuffing attacks, and these attacks result in an average of more than $6 million a year in costs per company. [1] At Auth0, credential stuffing attacks account for, on average, nearly **half** of all login attempts using our platform.

[1] Ponemon, The Cost of Credential Stuffing

What are credential stuffing attacks?

The Open Web Application Security Project (OWASP) defines credential stuffing attacks as "the automated injection of breached username/password pairs in order to fraudulently gain access to user accounts."

Credential stuffing attacks are one of the most common types of large-scale cyber attacks. Twenty-nine percent of data breaches in 2019 involved the use of stolen credentials, [2] and 1.5 percent of all logins on the web involve previously breached credentials.[3]

The basis of credential stuffing attacks is password reuse. Many users reuse the same password across multiple online accounts. According to TeleSign, 71 percent of accounts use the same password as other sites. [4] If that username and password combination is leaked in one data breach, the attacker can then try it out on other sites to compromise an account.

> * *71% of accounts use the same password across multiple sites[5].*

The failure rate for these attempts is high, so attackers need large lists of credentials to successfully find vulnerable accounts. Sometimes these lists are leaked to the public, and other times, they are sold for thousands or tens of thousands of dollars on the Internet.

Once the attacker has a list of compromised credentials, the next step is to try them against the target sites. Because of the large number of credentials and low success rate, attackers rely on automation in order to try thousands upon thousands of logins. They will generally

[2] Verizon, *2019 Verizon Data Breach Investigations Report*

[3] Google and Stanford, *Protecting accounts from credential stuffing with password breach alerting*

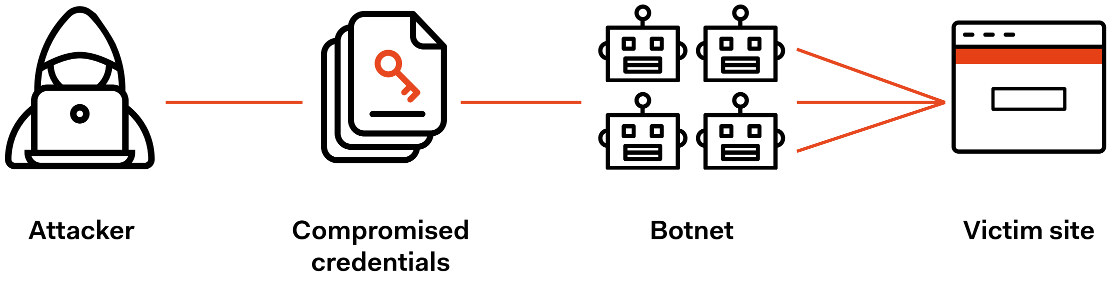
[4] TeleSign, *Consumer Account Security Report 2016*

[5] TeleSign, *Consumer Account Security Report 2016*

rely on standard web automation tools, such as Selenium or cURL, to handle the login attempts.

One of the challenges attackers face is rate-limiting and brute force detection by the victim website, which will prevent them from making a large number of login requests from the same IP address. To combat this, attackers typically rely on various tools and services to make the requests from a large number of IP addresses. At Auth0, we see 40,000 unique IP addresses involved in credential stuffing attacks every day. Once the attacker has secured a way to reliably test their credential list against the victim site, it is just a matter of time until the attacker finds all of the vulnerable accounts.

Anatomy of a credential stuffing attack

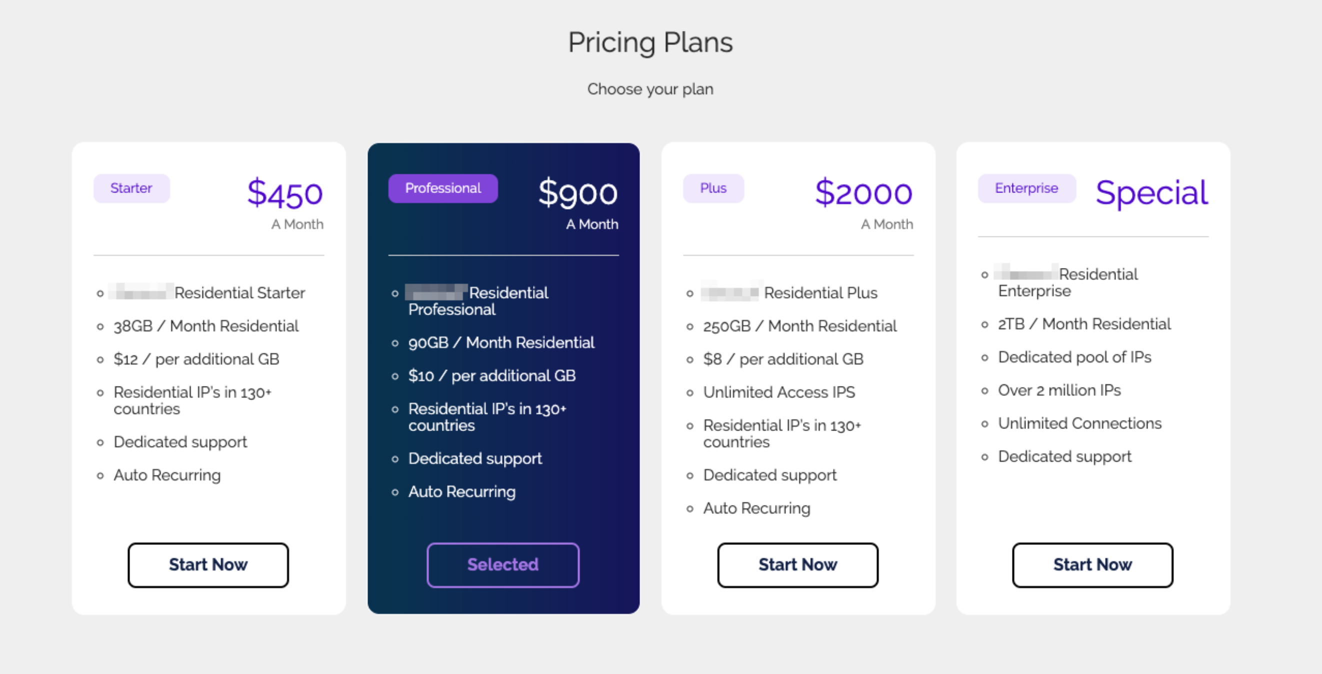


Credential stuffing attacks are easier than ever

The barrier to entry for conducting credential stuffing attacks is low – arguably lower than it has ever been before – and the potential payoff is high, because monetizing compromised accounts is simple.

The first part of the attack, password lists, becomes more prevalent as more breaches happen. The first half of 2019 had 54 percent more reported data breaches than the same time frame the previous year.[6] In addition, credentials are the second-most common type of data compromised in breaches, only behind internal company information.[7] More troubling, large aggregated lists featuring billions of username and password combinations, such as the Collections #1-5 lists, have started to appear.[8] All of this means it is easier than ever for attackers to obtain lists of credentials.

Rotating IP proxy services are cheap and easy to use



Pricing Plans

Choose your plan

Starter
$450
A Month

- [redacted] Residential Starter
- 38GB / Month Residential
- $12 / per additional GB
- Residential IP's in 130+ countries
- Dedicated support
- Auto Recurring

Start Now

Professional
$900
A Month

- [redacted] Residential Professional
- 90GB / Month Residential
- $10 / per additional GB
- Residential IP's in 130+ countries
- Dedicated support
- Auto Recurring

Selected

Plus
$2000
A Month

- [redacted] Residential Plus
- 250GB / Month Residential
- $8 / per additional GB
- Unlimited Access IPS
- Residential IP's in 130+ countries
- Dedicated support
- Auto Recurring

Start Now

Enterprise
Special

- [redacted] Residential Enterprise
- 2TB / Month Residential
- Dedicated pool of IPs
- Over 2 million IPs
- Unlimited Connections
- Dedicated support

Start Now

[6] Risk Based Security, *2019 MidYear QuickView Data Breach Report*

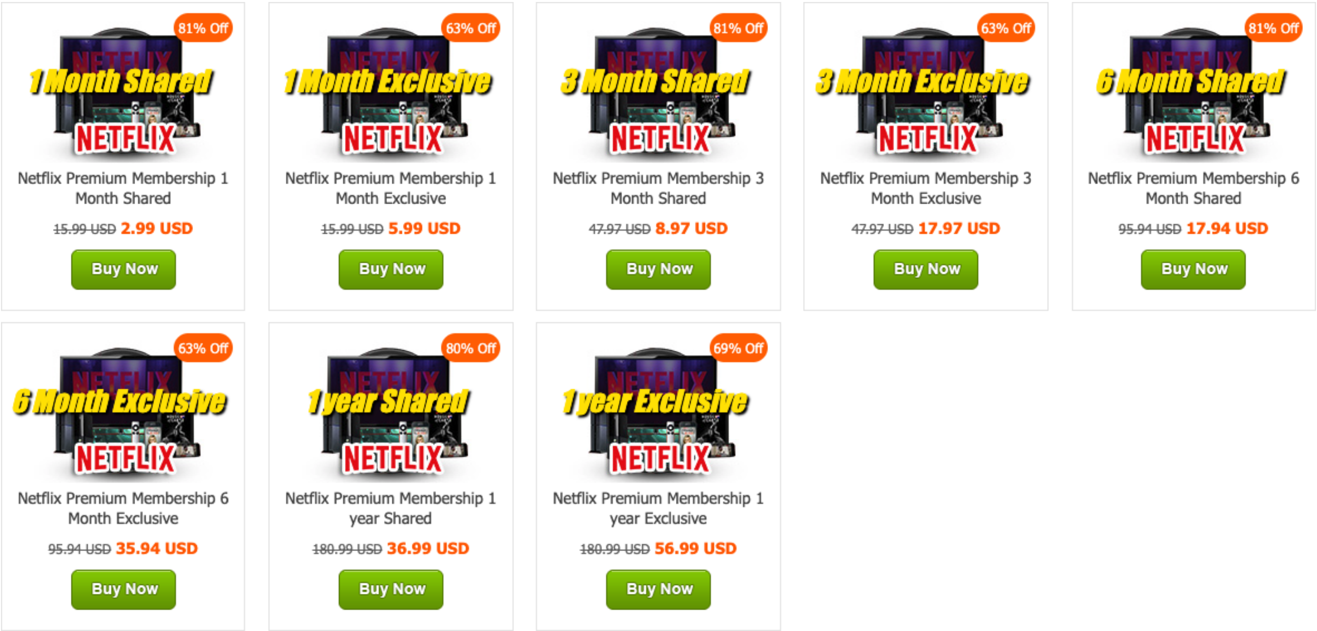
[7] Verizon, *2019 Verizon Data Breach Investigations Report*

[8] Wired, *Hackers Are Passing Around a Megaleak of 2.2 Billion Records*

In addition, the rotating IP proxy services are cheap and plentiful, which helps attackers circumvent rate-limiting and web application firewall protection. These services can be purchased for anywhere from $30 to $2000 per month and provide millions of rotating IP addresses.

There are many ways to monetize the compromised accounts. The simplest way is to just resell the compromised accounts on the Internet, but there are other more profitable and creative ways attackers will make money from credential stuffing attacks. Oftentimes, attackers will target streaming services that they can then resell on third-party sites for a fraction on the subscription costs. Another interesting scam is "sneaker botting." Attackers use compromised retail accounts to quickly purchase limited edition, high priced sneakers that they can resell for a profit. Conversely, if an attacker compromises a corporate employee account, they can use it to steal intellectual property and other company secrets.

Reselling streaming accounts is simple and profitable



Netflix Premium Membership 1 Month Shared
~~15.99 USD~~ 2.99 USD

Netflix Premium Membership 1 Month Exclusive
~~15.99 USD~~ 5.99 USD

Netflix Premium Membership 3 Month Shared
~~47.97 USD~~ 8.97 USD

Netflix Premium Membership 3 Month Exclusive
~~47.97 USD~~ 17.97 USD

Netflix Premium Membership 6 Month Shared
~~95.94 USD~~ 17.94 USD

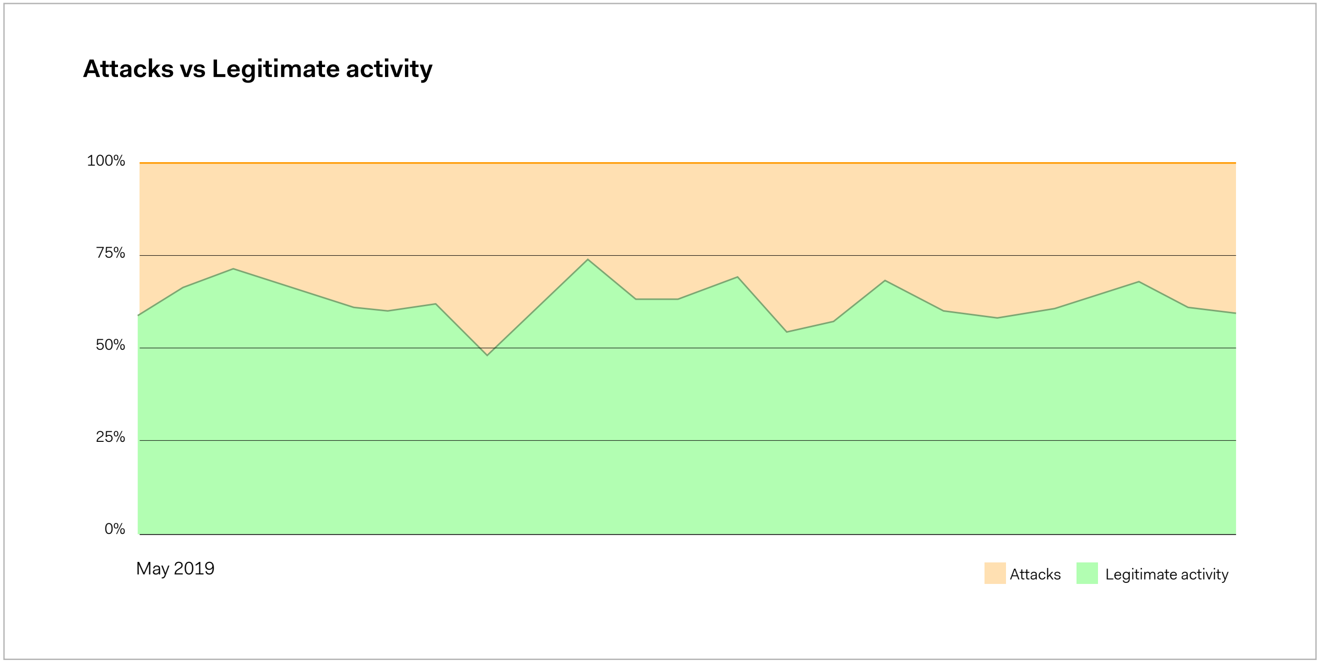
Netflix Premium Membership 6 Month Exclusive
~~95.94 USD~~ 35.94 USD

Netflix Premium Membership 1 year Shared
~~180.99 USD~~ 36.99 USD

Netflix Premium Membership 1 year Exclusive
~~180.99 USD~~ 56.99 USD

How credential stuffing attacks impact Auth0

As an IDaaS provider, Auth0 is often in a unique position to observe, detect, and combat credential stuffing attacks. These attacks are the most common type of attacks we observe targeting our customers. On a typical day, credential stuffing attacks make up nearly half of all login requests made to Auth0.



These attacks originate, on average, from more than 40,000 different IP addresses. This indicates simple rate-limiting and brute force protection won't stop every credential stuffing attempt. We've noticed some additional patterns in these attacks. Nearly all of the attacks we detect appear to originate from botnets, which are networks of exploited hosts that attackers can use to direct large-scale attacks in a coordinated manner.

Some attacks come in rapid bursts of a few dozen or hundreds of login attempts in very short periods of time. This is a quick method of conducting credential stuffing attacks, but it is "noisy" and typically easier to detect.

In other cases, we see far slower attacks where one or two logins are attempted every few minutes across a large number of hosts. These attacks come and go periodically and tend to fly under the radar compared to quick, high volume attacks.

Attackers will also try to periodically inject known valid credentials into the stream, resulting in successful logins. This tactic makes the activity appear more legitimate than if all of their attempts were unsuccessful. It also alerts the attacker if an IP address has been blocked if the login fails.

How to combat credential stuffing attacks

The first line of defense against credential stuffing attacks is Auth0's Anomaly Detection feature, which has two primary capabilities:

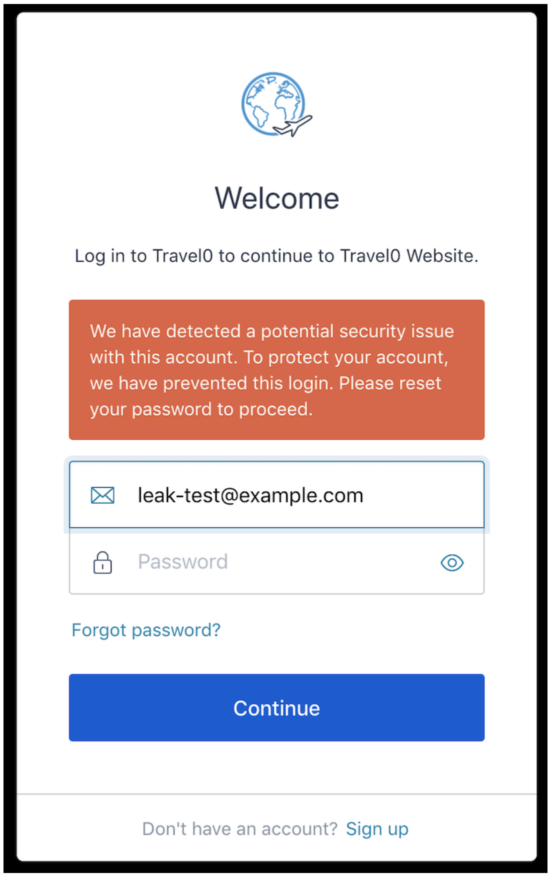
Brute force protection

This capability can prevent attackers who cycle through password combinations rapidly. It is triggered on 10 consecutive failed login attempts for the same user and from the same IP address, 100 failed login attempts from the same IP address in 24 hours, or 50 signup attempts per minute from the same IP address.

Breached password protection

This capability aims to identify users that are logging in with credentials that were known to have been breached and leaked to the public. Auth0 keeps a large, constantly growing database of username-password pairs that were known to be compromised in data breaches. Auth0 customers can choose to run all logins against this database to determine when users are logging in with compromised credentials.

When users are detected using compromised credentials, a number of actions can be performed. An admin can be informed while still allowing the login, the user can be prompted for multi-factor authentication (MFA), or the user can be blocked until they perform a password reset.

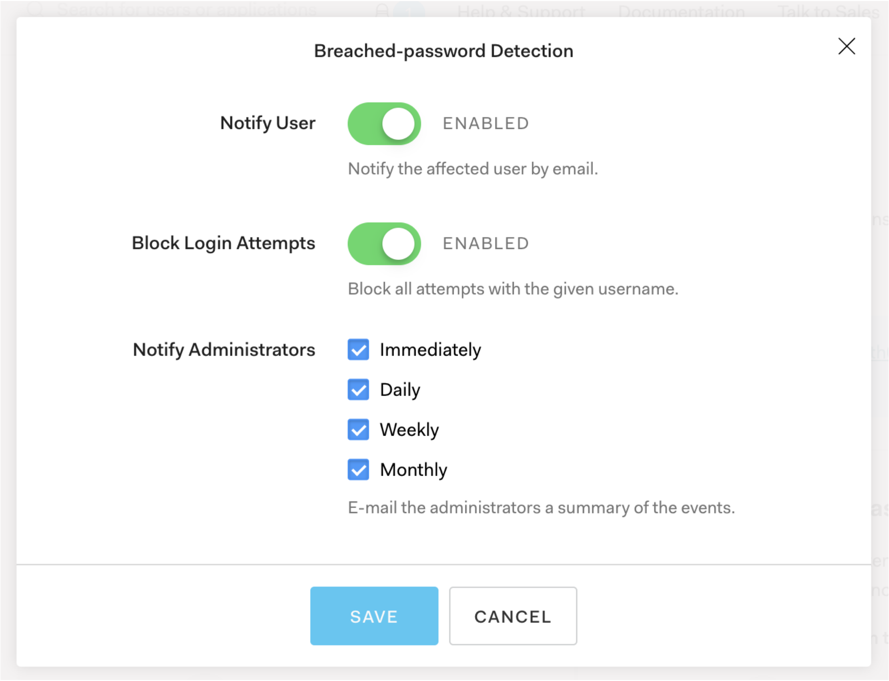


Welcome

Log in to Travel0 to continue to Travel0 Website.

We have detected a potential security issue with this account. To protect your account, we have prevented this login. Please reset your password to proceed.

leak-test@example.com



Breached-password Detection

Notify User: ENABLED

Notify the affected user by email.

Block Login Attempts: ENABLED

Block all attempts with the given username.

Notify Administrators

☑ Immediately
☑ Daily
☑ Weekly
☑ Monthly

E-mail the administrators a summary of the events.

Multi-factor authentication will stop most credential stuffing attacks

MFA is one of the best ways to prevent account takeovers, whether from a credential stuffing attack or something else. In order to compromise an MFA-protected account, attackers would need access to a set of breached credentials and the device used for the second factor. Overcoming MFA drastically increases the time and effort needed for the attacker to compromise the account, which makes it infeasible to do at scale.

The key here is to make MFA as easy as possible to enroll and use in order to promote adoption among your user base. Security doesn't have to mean a poor user experience.

Auth0 provides a variety of easy-to-use, friction-free MFA options. You can choose the MFA option that is right for your users – SMS, one-time password, third-party authenticators such as Google Authenticator, and more. Or choose Guardian, Auth0's proprietary MFA app, and let your users authenticate with the tap of a button.

Guardian facilitates MFA via push notification, enabling users to approve or deny login requests without ever opening the app. In addition to a better user experience, this is more secure when compared to SMS-based MFA, which is vulnerable to SIM swapping attacks. Guardian even works with Apple Watch or Android Wear.

The Guardian Mobile SDKs – available for iOS and Android – allows you to build your own white-label MFA app. This can be used to create a custom branded MFA app or embed MFA capability into an existing mobile app. If your mobile app already has a large installed base, you can deploy MFA functionality to all of them in an update, which means your users won't have to download a new app to enroll.

Use contextual MFA for a secure, easy user experience

You may not want to require MFA on every login to reduce friction. Using Auth0 Rules, you can define a wide variety of MFA scenarios. This spans from basic use cases, such as only prompting for MFA every *x* number of logins, to more advanced scenarios like enforcing MFA on logins from new devices or geolocations.

Step-up authentication is another common MFA scenario. It is a way to strike a balance between security and user experience. In this case, a user is able to log in initially without MFA. However, when the user tries to access a more sensitive function – to make a payment, for example – they are forced to complete MFA.

Anomaly Detection can also be combined with Guardian MFA for a low-friction way to combat credential stuffing attacks. When this is configured, users can log in normally without MFA, but if they are using a known breached password, they need to complete MFA to successfully authenticate.

This ensures users only have to perform additional steps to authenticate when there is reason to suspect they are victims of credential stuffing or other attacks.

Interested? Learn more!

If you are interested in combating credential stuffing attacks with Auth0, reach out to sales@auth0.com. Or learn more about Anomaly Detection and multi-factor authentication.

Auth0

auth0.com