SpyCloud

Credential Stuffing 101

How these attacks work, why they persist, and what you can do to prevent them.

***The goal of credential stuffing** is to gain unauthorized access to as many user accounts as possible, take over those accounts, and perpetrate fraudulent activities.*

Introduction

In early 2020, attackers compromised over 160,000 Nintendo accounts. Around the same time, approximately 500,000 of Zoom users' login credentials were shared on the dark web. Activision, The North Face, and Marriott International made headlines as hundreds of thousands of their customers' data landed in the hands of bad actors. For Marriott, this exposure of 5.2 million accounts was particularly painful as the company was already recovering from a 2018 breach in which over 300 million customer accounts were compromised.

With so many people stuck at home during the pandemic, popular consumer services were all facing high demand. It was inevitable that they would face increased security threats as well. In many of these cases, each organization was quick to insist that their systems were not compromised. But users' accounts, and sometimes their financial details, were.

Rather than trying to break into corporate infrastructure, attackers took a simpler path. Rampant password reuse allowed them to log directly into hundreds of thousands of users' accounts, aided by automated crimeware. In the case of Nintendo, SpyCloud researchers discovered source code for one account checker tool that was custom-built to help criminals test stolen credentials against Nintendo logins, enabling attackers to access customer accounts and exploit saved payment methods to purchase in-game currency.

The crimeware behind these attacks can be highly sophisticated, but the attack method – known as "credential stuffing" – is frustratingly ubiquitous. Perhaps even more frustrating is the question of whose job it is to prevent this type of attack.

What Is Credential Stuffing?

Credential stuffing refers to the act of testing large sets of stolen credentials against targeted applications or web interfaces. Compromised credentials yielded from data breaches are used to build "dictionaries" or "combo lists." These credentials are traded and sold within criminal networks and then used for credential stuffing operations. In effect, as long as companies keep getting breached, the lists keep getting better.

One of the key components of credential stuffing attacks, a combo list is a list of previously breached credentials which are loaded into automated brute-force tools to test credentials against thousands of sites at a time. These tools can check for common password variations as well.

With each passing cybersecurity incident, promises are made by the victim organizations to identify the culprit(s) and ensure consumer protection. This strategy is flawed because we, the consumers, are a huge part of the problem. Analyzing all of our breach data, SpyCloud found

that among users who were exposed in two or more breaches, 57% reuse the same password (or small variations) across multiple accounts. Because of this, it's easy for attackers to use combo lists to unlock many accounts.

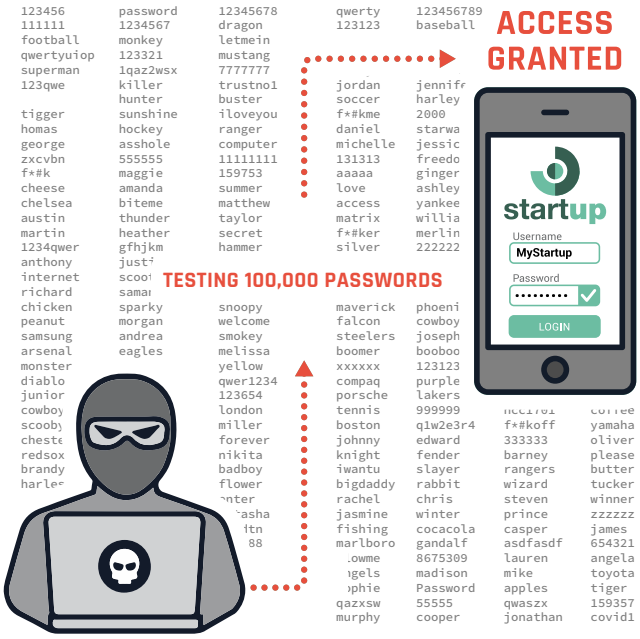
Gigantic troves of stolen credentials available on the dark web combined with automation make these attacks scalable and fairly straightforward. Using readily available crimeware, even unsophisticated cybercriminals can feed (or "stuff") millions of compromised credentials into the login pages of any number of websites at a time.

The goal of credential stuffing is to gain unauthorized access to as many user accounts as possible, take over those accounts, and perpetrate fraudulent activities. Account takeover (ATO) enables attackers to drain money from bank accounts, make large purchases, steal identities, or combine real and fake information to create new "synthetic" identities. The 2020 SolarWinds supply chain attack offers a worst-case scenario: an attacker who escalated user privileges to gain a foothold in an organization's network and carried out serious, long-term, and costly attacks.

In SpyCloud's 2021 Annual Credential Exposure Report, we stressed the importance for enterprises to distinguish between whether consumer accounts have been accessed due to a breach of internal resources or via credential stuffing.

> ***A breach results from a company's failure to protect its assets and often has regulatory implications, whereas credential stuffing is typically the result of consumers' bad password hygiene.***

But how much responsibility do organizations shoulder for users' password choices? With consequences including brand damage and loss of customer trust, more businesses are taking a proactive security stance – alerting customers when their credentials are compromised in a third-party breach (not of their own site, but of another site altogether) because passwords are so commonly reused across accounts. A breach of one service can have cascading effects on other businesses, particularly when it comes to credential stuffing.



What Makes Credential Stuffing Possible?

Password Reuse
On average, people are expected to keep track of around 70-100 passwords. It's not surprising that an analysis of SpyCloud's database revealed an all-time password reuse rate of 57% – and a 60% password reuse rate for breaches collected in 2020. The problem is only getting worse.

Gigantic Breaches
2005 saw the first data breach of over 1 million records, which was startling at the time. They kept getting bigger; eight years later, the Yahoo data breach exposed an astonishing 3 billion records. Today, it's common for breaches to result in tens of millions of exposed credentials. These username + password combinations form the basis of combo lists, a key component of credential stuffing attacks.

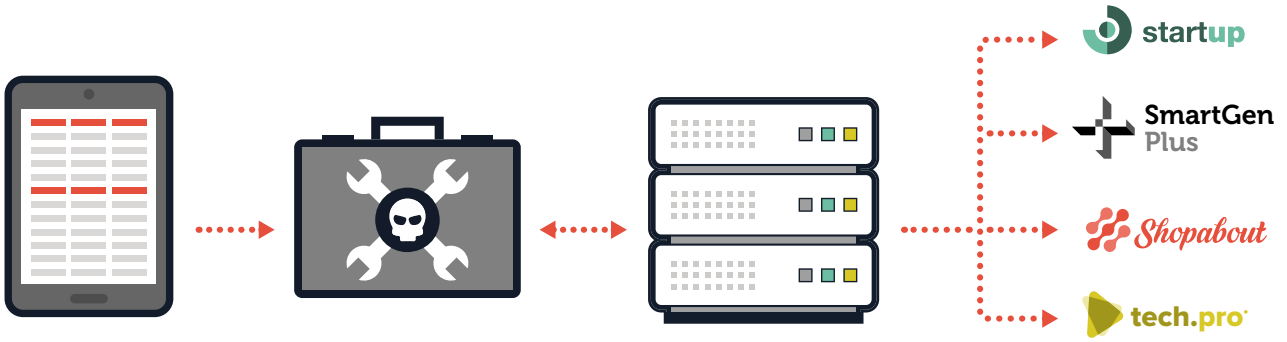
Automation + Low Barrier to Entry
Credential stuffing is a numbers game — and a profitable one. Thanks to automation, even a small-time criminal can test 100,000 credentials for less than $200. The typical success rate is low, between 1-2 percent, which means the attacker can net up to 4,000 valid accounts from a single attack starting with 100k credential pairs.

Sluggish Detection
The average time for an organization to identify and contain a breach is 280 days. This gives attackers a big window to abuse stolen credentials.

The Anatomy of Credential Stuffing Attacks

Criminals do not literally type in hundreds of thousands of credentials across multiple sites by hand. Furthermore, web services have limits in place to block any flood of activity coming from a single IP address. If credential stuffing attacks had to be done manually, they would not be feasible or profitable, so automation is key.

Automated credential stuffing tools are available for purchase at relatively low cost on malicious platforms. Rather than writing automation scripts themselves, many attackers use so-called "account checkers." These tools make it easy for attackers to feed in a huge list of stolen username and password pairs and test them on targeted sites.



A typical credential stuffing scenario for a criminal works like this:

1. **Buy a Combo List**
In the past, skilled attackers had to break into sites to steal credentials. But today, so many valid credentials are already available on the dark web that even unskilled attackers can easily obtain them. A criminal can purchase a combo list that combines data from multiple breaches from an underground market for as little as $2.

2. **Get In Disguise**
To be successful, credential stuffing attacks must appear like regular network traffic on the targeted website. Millions of login requests suddenly coming from a single IP address in a short time period would raise red flags with defenders. To avoid this, an attacker can enlist the help of IP proxy service providers that use bots to distribute login requests across thousands of IP addresses, thus helping to hide suspicious attacker activity.

3 Load List and Analyze Accounts

Public resources enable criminals to quickly download a tool that compares combo lists against popular commercial websites. The criminal will load the combo list into the tool and can select certain sites simply by checking the boxes for each site or can run the tool against hundreds of sites at once. Criminals can even custom-configure credential stuffing tools to find accounts with certain balances of cash, points, and/or virtual currencies. When there's a match, they'll see account balances behind compromised accounts and determine ahead of time whether or not they can gain access to the targeted account.

4 Launch Attack

The attacker's objective is to uncover all successful login requests. As the tool runs through the supplied credentials, the attacker is notified of valid ones. Technically, the attack itself is complete when the attacker receives these results. But simply obtaining a list of valid credentials is not the attacker's end game.

5 Begin ATO

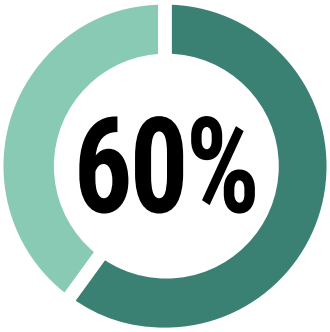
Armed with a list of validated credentials for a target site, the attacker will pivot to monetization. How they accomplish this depends on their objective and the type of site attacked. The goal is to drain accounts of their value, so they might steal funds through fraudulent banking transactions, make large purchases on e-commerce sites, take cash advances against credit cards, or liquidate gift or rewards cards for cash or products. More sophisticated attackers use legitimate accounts to gain deeper access into a victim's network, escalating privileges to carry out more sinister acts like shutting down infrastructure or stealing company information or trade secrets.

The Impact of Credential Stuffing

- According to a Private Industry Notification issued by the FBI last year, **credential stuffing accounted for 41% of security incidents against the US financial sector between 2017 and 2020.**
- Excluding costs associated with fraud, **credential stuffing costs affected businesses an average of $6 million per year.**

Regardless of your industry, credential stuffing is an equal-opportunity offender and the implications are very real. In 2020, a mid-sized U.S. financial organization linked a flood of login attempts using various credential pairs to more than $3.5 million in fraudulent transactions. Even where there is no actual fraud committed, credential stuffing can still have an impact. From June 2019 to January 2020, a NY-based investment firm was hit with credential stuffing attacks against their mobile APIs, resulting in a system outage that blocked the collection of nearly $2 million in revenue.

Fraud losses aside, these reports say nothing about the possible legal costs and regulatory fines that could result, not to mention the loss of brand reputation and customer trust. Nearly 50% of consumers in a CA Technologies survey said they stopped using a company's services because of a data breach – and these days, data breaches and credential stuffing attacks are perceived as nearly one and the same.



of users reused at least one password across more than one account *according to SpyCloud's 2021 Annual Credential Exposure Report*

Preventive Measures

Much like phishing or downloaded malware, credential stuffing relies on the weak link in every organization – people. Any preventive action against credential stuffing has to begin with people and their passwords.

- **Strengthen Passwords**
  Enforce strong password policies using NIST guidelines. In particular, ban commonly-used passwords, including passwords that are known to have been in a breach. For employees, consider implementing an enterprise-level password manager and encouraging them to leverage it for personal accounts.

- **Implement MFA**
  Implement multi-factor authentication (MFA) for as many of your public-facing websites as possible, as well as for internal resources that handle sensitive and confidential data. While it's not foolproof protection (attackers constantly seek out new techniques to thwart defenses) it provides an obstacle that may not be worth the effort to defeat for criminals looking to profit from low-effort credential stuffing attacks.

- **Automate Prevention**
  Automation is key, with logins checked seamlessly for compromise behind the scenes. Even if the criminal is able to find exposed passwords from a breach that work on other sites, they won't be able to use them to access yours – if you are proactive about forcing password resets for users who have been compromised in a third-party breach. There are ways to implement these measures without hindering legitimate user activity.

Conclusion

It's no secret that attackers will take advantage of "low-hanging fruit" — the lowest-effort, highest-payoff stuff. As long as there are criminals willing to pay for stolen data, consumers failing to protect themselves, and businesses fearful of introducing a small amount of friction in the service of protecting users (and their bottom line), there will be credential stuffing attacks. With record numbers of people working from home as well as shopping online, creating new accounts and reusing passwords, this massive problem will only intensify.

The hope is that both consumers and organizations will be proactive and take the precautions available to them. For consumers whose habits are hard to break, so as long as we keep reusing passwords, we can expect credential stuffing attacks to persist.

Security professionals owe it to themselves and to each other to force better password hygiene, monitor for compromise, and take action when it happens. In our interconnected world, where so many platforms and technologies intersect, compromises of one service can easily cascade into losses for others.

The SpyCloud Difference

Building a security program around technologies that proactively leverage data acquired through Human Intelligence (HUMINT) tradecraft very early in the breach timeline is a critical path to success. SpyCloud's solutions, backed by the world's largest repository of recovered stolen credentials and PII, enables enterprises to stay ahead of both targeted account takeover and credential stuffing by detecting and automatically resetting compromised passwords early, before criminals have a chance to use them.

Our customers continue to tell us their ability to prevent account takeover hinges both on access to relevant data (including the most plaintext passwords in the industry) and in being able to make that data operationally actionable through automation.

See Your Account Takeover Risk →

Discover how many breach records are associated with your email address and your domain as a whole. Once you know, you can take action.

Consumer ATO Prevention

Protect your users from account takeover fraud and unauthorized purchases.

Learn More →

Employee ATO Prevention

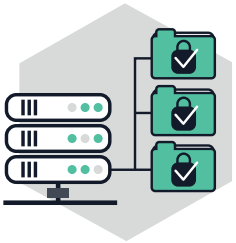
Protect your organization from breaches and BEC due to password reuse.

Learn More →

VIP Guardian

Protect your highest-risk executives from targeted account takeover.

Learn More →



Active Directory Guardian

Automatically detect and reset exposed Windows accounts.

Learn More →

Third Party Insight

Monitor third party exposures and share data to aid in remediation.

Learn More →