SpyCloud

Account Takeover 101

What Is It & What Can You Do to Prevent It?

1

Jon reuses his password on his social network, bank, favorite ecommerce store, and your site

Across the SpyCloud database, we've found that 60% of users exposed in more than 1 data breach are reusing passwords across multiple account

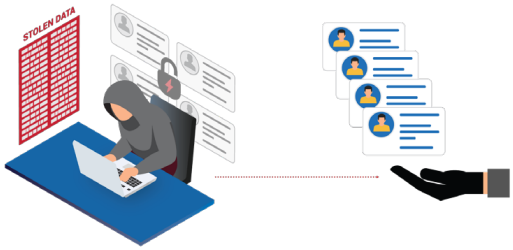
2

His bank is breached

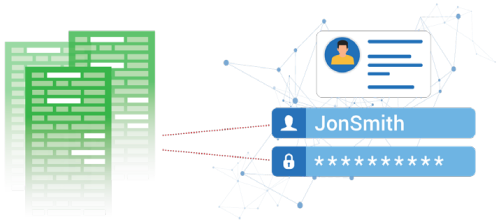
3

A small circle of threat actors trades the bank's user credentials in the underground

This is typically when SpyCloud recaptures the data and makes it available to our customers so they can flag accounts and reset passwords – preventing ATOs!



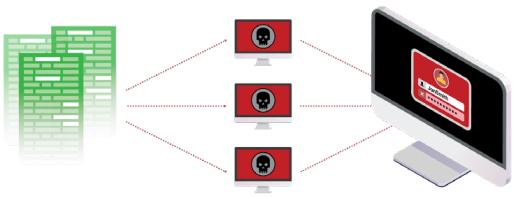
4



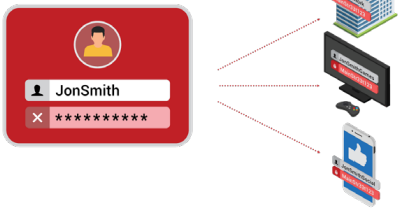
Eventually, the username / password pairs are loaded into new combo lists for sale on dark web markets

5

Threat actors use the combo lists in credential stuffing attacks against your website that take advantage of people's tendency to reuse passwords



6



Jon's account is compromised with his reused username & password, resulting in account takeover, fraud, support calls, and brand damage for your site

As criminals up the ante in the cybercrime war, it is critical for all of us to understand how these attacks work and what you can do to ***prevent your enterprise, and yourself, from becoming a victim.***

Introduction

Among the most alarming trends in cybercrime is the overwhelming surge in account takeover (ATO) attacks. While criminals have for years made a very lucrative business out of selling the data from compromised accounts to fraudsters who, in turn, used it to commit crimes against financial, retail, and other digital services, the threat of ATO wasn't well known outside of security circles.

The arrival of the COVID-19 pandemic changed that completely. Within a short period of time, our culture dramatically shifted how it viewed the digital world. From the uptick in online banking to the proliferation of accounts we created for streaming and food delivery services to our necessary "work-from-home" tools, embracing all-things-digital allowed us to maintain some semblance of normalcy and keep many businesses afloat. It also greatly expanded the attack surface. This global event, combined with automated technologies, resource-strained security departments, and a spike in unwitting, vulnerable consumers created a virtual playground for ATO.

Even if you're familiar with ATO and think you're prepared, the truth is that ATO is a never-ending game of whac-a-mole; as soon as one hole in your security program has been plugged, another appears due to human error or criminal ingenuity.

SpyCloud has been at the forefront of addressing the myriad challenges businesses and consumers face as they scramble to address escalating ATO threats while at the same time ensuring seamless customer experiences that don't introduce unnecessary friction. As criminals up the ante in the cybercrime war, it is critical not only for businesses, but all of us, to understand how these attacks work and what you can do to prevent your enterprise, and yourself, from becoming a victim.

Account Takeover: What Is It?

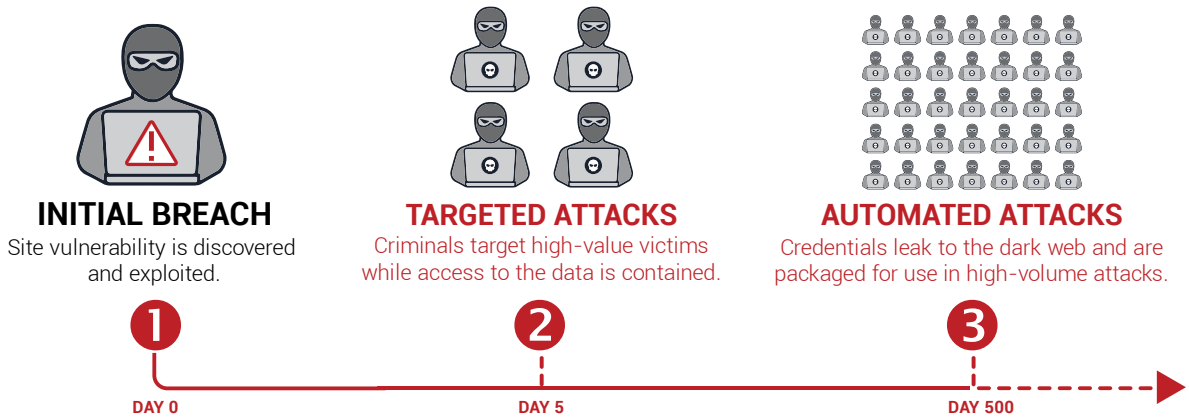
If a stranger asked you to provide them with your username and password for any of your online accounts – whether corporate or personal – it would certainly raise a red flag, right? People are increasingly aware how important it is to keep their login details, data, and files confidential. However, these situations are rarely that cut-and-dry. Cyber attackers don't request access to your digital accounts; they take them, along with your money and personal data, any way they can.

In an account takeover attack, criminals use another person's login credentials, most often by leveraging reused or similar passwords from previously breached sites, to gain access to existing accounts. Once inside, they make unauthorized transactions, siphon funds, and steal corporate data or personally identifiable information (PII) to use for other purposes, or simply to sell to other attackers on the dark web.

ATO is a scary and dangerous threat with the potential to inflict significant financial harm on businesses and individuals. With so many entry points into cloud-based systems and networks, ATO presents one of the greatest risks to our digital world. Criminals don't need to use sophisticated technologies to breach firewalls or other security measures intended to protect the enterprise. They just need your password.

Even with all of the security measures businesses put in place to prevent these attacks, the needle is moving in the wrong direction. In 2019, ATO was the top fraud method with a 72% year-over-year increase on financial accounts alone. In 2020, with COVID-19 disrupting our world, the year-over-year growth was startling – over 300%.

Account Takeover Timeline



There are 3 main phases in the lifecycle of an ATO attack. You are likely well aware of the initial phase – the data breach that is the impetus for stolen data to get into criminals' hands. What you may not know is that breaches can happen months and even years before they make the news. What is happening during that time?

1 Phase 1: The Breach

The first step for criminals is to find and exploit vulnerabilities in websites and apps to gain access to their user database. A breach can impact thousands of users at a time, exposing not only their passwords, but even more sensitive information like account questions/answers, dates of birth, and phone numbers that can be put to use in follow-on attacks.

2 Phase 2: Targeted ATO Attacks

During this time, the stolen data are high-value assets. Criminals are not yet turning to the dark web to sell them; instead they keep the stolen information contained within their trusted network until they've fully monetized it, which can take as long as 24 months. The attacker might engage trusted advisors to help them parse the data and crack passwords. They may target an organization they have a specific interest in, and identify VIPs with high levels of systems access, or exceptionally wealthy or high-profile victims who should be treated differently than the rest, and get creative in targeting them with manual account takeover. These tactics can be complex and hard to detect, and result in huge losses. In fact, SpyCloud customers report that 80% of losses come from 10% of ATO attacks, which are considered highly targeted. Having access to stolen data early in the breach timeline gives organizations a major advantage, enabling them to identify and reset compromised credentials before criminals have a chance to use them.

Get a deep dive on targeted attacks →

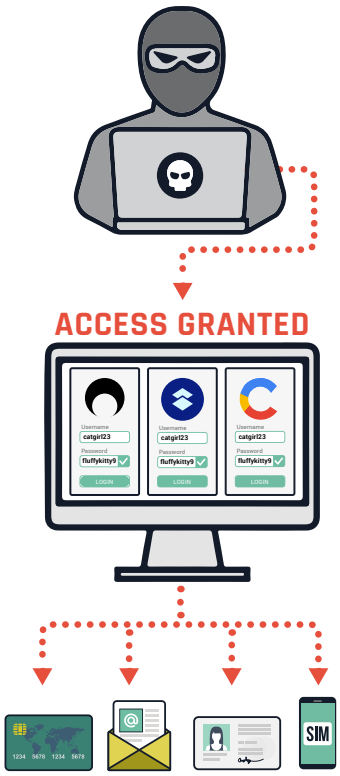
3 Phase 3: Automated ATO Attacks

Having extracted as much value out of the stolen data as possible, the next step is to package it for sale to less sophisticated criminals, who can automate credential stuffing attacks with minimal effort, expense or expertise. Criminals know we commonly reuse the same password across different accounts, and credential stuffing is a type of brute-force attack that exploits this. It leverages automated, cheap, and easy-to-use tools to test large volumes of stolen usernames and passwords across multiple sites until one works. Even very old credential data can still yield results.

The Consequences of Account Takeover

Criminals are typically taking over accounts for profit, pure and simple. It all comes down to money, and how much of it criminals can extract from what they've stolen. Contrary to what you may have heard elsewhere, the first step to monetizing stolen data is not to sell it on the dark web. That's actually the *last* step. What happens first is the highest effort, most profitable activities.

With stolen data, criminals will:



- **Drain financial accounts, crypto wallets or loyalty point balances**
  Criminals will take control of financial accounts and immediately wire or transfer the balance from victims' accounts. In a twist on this concept, there has been a huge uptick in peer-to-peer payments fraud, up 733% since 2016.
- **Make fraudulent purchases**
  Another quick scheme: criminals will purchase goods using stolen or stored credit card or gift card data. In fact, 40% of all fraudulent activity associated with an account takeover occurs within a day.
- **Create synthetic identities**
  Some criminals are specialists when it comes to creating new identities with a combination of fake and legitimate (stolen) data. The payoff might not come for months, since these identities need to be "warmed up" before they are used to obtain lines of credit.
- **Exploit victims' work accounts**
  Criminals may try to locate and steal corporate IP and deploy business email compromise scams, which resulted in $1.7B in losses in 2019 alone.
- **SIM swap victims to bypass MFA**
  In a SIM swap attack, criminals transfer a victim's phone number to their own SIM card in order to bypass multi-factor authentication and take over sensitive accounts.

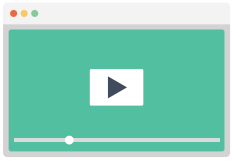
Once maximum value from the data has been extracted, only then is it packaged up for sale on the dark web.

"Fullz" are desirable, giving criminals everything they need to commit identity fraud for $8-10; ***however, when financial information is included, the criminal can command a 10x+ higher price.***

The Value of Stolen Data

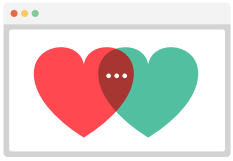
How much your data is worth to other criminals varies quite a bit. Full packages of information on individuals (known as "fullz") are desirable, giving criminals everything they need to commit identity fraud – typically name, national ID number, date of birth, and specific account credentials for $8-10 according to our own research and those of others in our space; however, when financial information is included, the criminal can command a 10x+ higher price.

For account credentials alone, let's take a look at some representative average pricing for common account types, based on SpyCloud's analysis of an estimated 308,214 transactions across 800 criminal shops on 3 prevalent ecommerce platforms in November & December 2020:

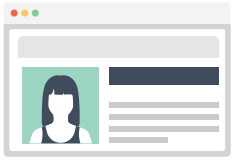


Streaming account
$4.54

Gaming account
$6.05



Dating account
$5.18



Professional software account
$2.94

Chain restaurant loyalty account with points:
$1.25

Home goods ecommerce account with $500- $950 credit balance:
$64

Ecommerce clothing retailer account with £2000 credit balance:
$161.73

Bad Habits That Increase ATO Risk

Buried in each phase of the attack cycle are common habits we are all guilty of. To criminals, these habits are akin to leaving your spare house key under your front doormat: totally obvious. In other words, our online habits make us really easy marks. Likewise, for each common bad habit, criminals use their own common strategies and tools to their advantage.

BAD HABIT	HOW CRIMINALS EXPLOIT IT
We Choose Weak, Common Passwords Regardless of all the advice out there about the importance of strong passwords, users will choose sequential numbers and dictionary words or add a ! or 1 to the end of their password (especially when prompted to change passwords every 90 days by corporate IT). Memorable passwords may seem unique to users – but they often aren't. Among the millions of passwords SpyCloud recovered from breaches last year alone, "123456789" was found over 35 million times. "querty123" was found over 13 million times, "iloveyou" 3 million times, and "football" 1 million times. Unless these passwords are banned and password complexity requirements put in place, some users will always select easy-to-remember passwords.	**Password Spraying Attacks** Easy-to-remember passwords are also easy for bad actors to guess, making consumers vulnerable to password spraying. Password spraying is a brute force attack where a cybercriminal uses a list of usernames and common passwords to try to gain access to a particular site. Once they get a match, they'll test that same username and password combination against as many accounts as possible. There are plenty of news stories about admin passwords that contain the company name. It's actually a huge problem that we've come across too many times to count in analyzing the SpyCloud breach database, and something we recommend customers include on their list of banned passwords.
We Reuse Passwords Across Multiple Accounts In a Google study, 66% of people admitted to reusing the same password across one or more accounts. SpyCloud's own research shows that even employees at some of the world's largest and most innovative companies share this bad habit; over 76% of Fortune 1000 employees are reusing passwords across work and personal accounts. When one site is breached, cybercriminals can access any other accounts that are protected by the same credentials. Using a password manager is a way to kick this habit, but only some flag compromised passwords and stop users from choosing them.	**Credential Stuffing Attacks** Credential stuffing makes it possible for criminals to profit from even very old breach data that they buy on the dark web and successfully take over multiple accounts. Credential stuffing tools let criminals test credential pairs against a number of websites to see which additional accounts they can take over; hence why password reuse is so dangerous. Some criminal tools can even test for common password variations, like changing certain letters to numbers (Password vs. P@ssw0rd) or adding numbers or symbols to the end of a word (password123). If a password has been exposed in one data breach, any other account with a variation of the same password is at risk.
We Click Links & Download Attachments from Unfamiliar Sources To the dismay of security teams everywhere, users habitually click any link or file that lands in their inbox, whether they recognize the sender or not. Inevitably, this leads to users' machines becoming infected; 94% of malware is delivered by email! Some malware can harvest usernames and passwords, browser cookies, autofill data, and more – putting those users at extremely high risk of ATO.	**Keylogger Malware** There are sites available on the dark web to purchase all the tools and services criminals need to launch malicious campaigns – the malware itself (yes, there's even 'malware-as-a-service' now), hosting infrastructure, phishing kits, and spam service. It's all aimed at making it very easy for users to fall for these schemes. Malware with keylogging components can record a user's every move, and criminals will use the data for all manner of malicious purposes.

Preventing Account Takeover

For businesses, combating account takeover attacks requires dedicated detection and mitigation techniques. Considering the hyper-speed at which automated technologies are fueling ATO, it's imperative that users remain educated on good security hygiene and put the information they learn into practice, while businesses put layers of proactive solutions in place. Users and businesses working together is the only way to disrupt the criminal's ability to profit from stolen information. While organizations may not be able to prevent every breach or every ATO, when and how they respond to these threats will dictate how much they may lose.

Early Detection and Fast Remediation

This can't be stressed enough. For security teams, the key to preventing ATO is to identify compromised accounts early, before criminals have time to exploit them. The only way to do that is to have access to a comprehensive, constantly updated, real-time database of breach data. No single security team can validate and remediate compromises at the speed necessary to narrow the exposure window to days, instead of months or years (when stolen data is finally leaked to the dark web and widely available to those looking for it). The best method to get ahead is to work with specialists in the field of breach data collection; one that combines automated technologies with human intelligence to gather breached data as early as possible in the attack timeline, and make it machine-friendly and actionable.

NIST Password Security Compliance

For organizations, controlling users' bad password habits poses a major challenge. With the human factor in mind, the National Institute of Standards and Technology (NIST) has provided concrete, user-friendly password guidelines that encourage strong passwords:

NIST

- **Previous breach exposures**
- **Less than 8 characters**
- **Context-specific words**
- **Dictionary words**
- **Repetitive characters**
- **Password hints**

Aligning your enterprise's password policy with the latest guidelines from NIST can certainly help encourage better password habits and reduce the risk of ATO. You can enforce many of these guidelines through the built-in settings provided by most directory services, including Microsoft Active Directory, while for others, a layered solution may be necessary.

Taking Charge of Your Own Security Hygiene

Without access to the high-tech monitoring and detection tools available to corporate security teams, individuals can often feel defenseless against ATO. This doesn't have to be the case. Today's security leaders have stepped up to educate employees on good security habits, and those same principles can be applied to personal accounts. Using unique, complex passwords with at least 16 characters, symbols, and numbers for each account is something no one wants to manage (which is why password managers exist!). But ATO is proving to be a hugely disruptive force that knows no limits. Your passwords may be nearly impossible to remember, but they will also be nearly impossible for threat actors to guess.

Furthermore, stop clicking on links if you don't trust the source – this applies to mobile devices (one of SpyCloud's leaders jokes about how he doesn't even trust links his wife texts him but... he really doesn't!).

Myth-Busting Your ATO Prevention Strategy

As soon as the good guys think they've figured it out, the bad guys try something new. In other words, you might think you've got your bases covered, but most criminals are already one step ahead of you.

Many organizations lean too heavily on the 'status quo' of cybersecurity. Each of these layers of protection can play a role, but they are flawed in their own ways that are important to understand.

- **Multi-Factor Authentication (MFA)**
  Requiring users to provide something they know (a password) plus something they are (biometrics) or something they have (smartphone token), is an important layer of protection and will deter some cyber attacks. Some. Not all. It is still possible via many avenues to bypass MFA. More importantly, it causes friction between the user and the service. Most of us will buck at pulling out our phones to tap 'approve' on a login multiple times a day and may turn MFA off at the first opportunity.
- **Password Managers**
  Even when companies mandate their use, most employees don't use password managers at home or for personal services. This wouldn't be such a problem if password reuse wasn't so rampant and the lines between personal and employee accounts and devices weren't already blurred. Confusing BYOD policies and the use of employee accounts on personal devices only make the situation worse.

- **90-Day Password Rotation**
  Password rotation policies actually benefit threat actors more than the users. Criminals test stolen credentials on a regular basis knowing that eventually, the user will think they're safe and unknowingly reset their password to one that has already been compromised.

- **Behavior or Heuristic-Based Solutions**
  Many of these solutions have a machine-learning backend whose algorithms have been trained upon vast amounts of login and/or breach data. These algorithms, they claim, can detect a possible account takeover before it ever begins. Not true. Criminals perpetrating targeted ATO are using advanced tactics that are far less likely to tip off any AI that's been trained on automated ATO data.

- **Dark Web Monitoring**
  Most solutions in this category rely on scanners, crawlers and scrapers that troll dark web forums and pastebin sites for leaked credentials. Credentials that are for sale are almost never posted in their entirety in advertisements on dark web forums, the open web or any public environment that can be scanned. Bad actors usually post only a redacted sample of their credentials online to advertise their goods. The complete credential sets can only be obtained through vetted relationships with threat actors who sell and trade their fullz to trusted partners. It takes human analysts to find what's not as obvious.

Conclusion

Protecting individuals and organizations from ATO is a never-ending cat-and-mouse game and there is no single solution capable of making threats disappear. Criminals are clever and will keep inventing ways to steal from you, and on the whole, users will keep making mistakes that put their accounts at risk. As a corporate security team, you can't defend yourself alone. ATO prevention requires users to own their online security alongside your cyber programs and policies. As part of a strong cyber program, you need strong partners that specialize in staying ahead of evolving ATO attacks.

If there is one tool everyone should have in their arsenal, it's direct access to breached data. The ability to quickly identify compromised accounts, reset passwords, and block ATO from damaging your organization presents the rare thrill of beating attackers at their own game.