SpyCloud

Targeted vs. Automated **Account Takeover Attacks**

SpyCloud customers say

80%
OF LOSSES

come from just

10%
OF ATTACKS

Targeted vs. Automated Account Takeover

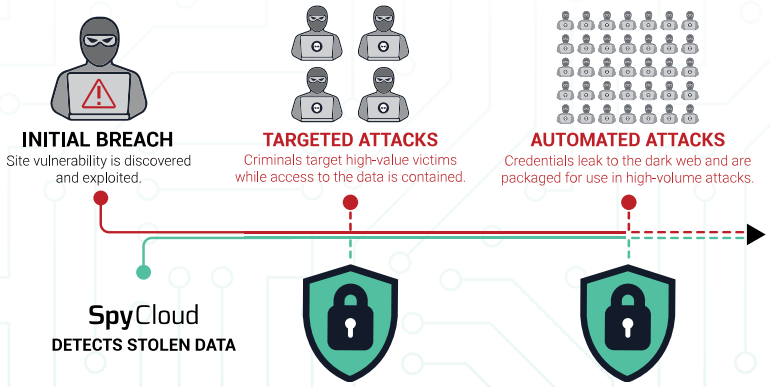
Account takeover (ATO) occurs when criminals use stolen credentials to access a user's accounts without permission, often in order to make fraudulent purchases, steal sensitive data, or move laterally within a target organization.

The vast majority of account takeover attempts are automated. However, SpyCloud customers report that 80 percent of losses come from just 10 percent of ATO attempts, which are highly targeted and challenging to detect. SpyCloud helps protect against both targeted and automated ATO by recovering stolen data early in the breach timeline, enabling organizations to reset compromised credentials before criminals have a chance to use them.

Protect Your Enterprise from Account Takeover at Every Stage of the Breach Lifecycle

After a breach occurs, criminals typically keep stolen data contained within a tight circle of associates while they determine how to monetize it most effectively. Because few people have access to the data, stolen credentials are valuable assets. This is when unsuspecting organizations and individuals are at the greatest risk of targeted attacks—and this is also when SpyCloud researchers gain access to breach data.

The attackers and their associates systematically monetize stolen data over the course of about 18 to 24 months before gradually allowing credentials to leak to more public locations on the deep and dark web. Once they become available to a broad audience, including dark web scraping and scanning tools, the credentials become low-value commodities. At this stage, passwords have been cracked and plaintext credentials have been packaged into "combolists," which are lists formatted for use with automated account checker tools that make credential stuffing easy and accessible for unsophisticated criminals.



Let's take a closer look at both types of attacks and see why targeted account takeover is often underestimated.

After a breach occurs, criminals typically keep stolen data contained within a tight circle of associates while they determine how to monetize it most effectively.

Targeted Account Takeover Attacks

Challenges for security teams:
Highly effective, difficult to detect, huge potential losses

Challenges for criminals:
Time-consuming, not scalable

Automated Credential Stuffing Attacks

Challenges for security teams:
Easy for unsophisticated criminals to launch high-volume attacks

Challenges for the criminal:
Easy to detect and prevent

Stage 1: Identify Targets

Focus on Specific Companies or Individuals

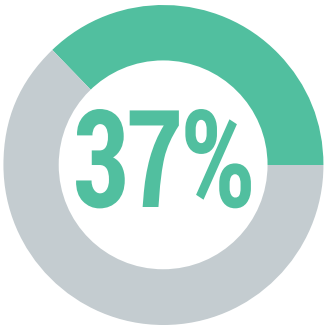
After a data breach, a criminal and their associates evaluate stolen information and prioritize certain high-value individuals and organizations for targeted, manual attacks. They may take steps such as:

- Profiling wealthy or high-profile individuals
- Identifying C-level executives or developers with internal access to valuable corporate assets
- "Fingerprinting" a particular target organization to pinpoint defense thresholds and optimize attack strategies

Target a Broad Range of Companies, Not Specific Individuals

A criminal engaging in automated credential stuffing attacks will target any company with active online accounts that they can attempt to take over and resell, trade, or otherwise monetize. Affected industries may include:

- Entertainment & multimedia services
- Food delivery
- Ecommerce and retail
- Travel and hospitality
- Education
- Professional software
- Healthcare



Of all data breaches in 2020, regardless of attack type, ***involved the use of stolen credentials.***

- 2020 Verizon Data Breach Investigations Report

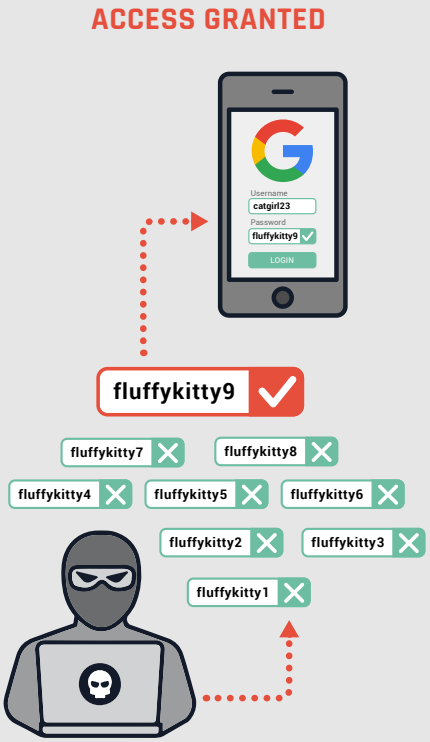
Stage 2: Aquire Data

Targeted Account Takeover Attacks

Research Targets and Find an Entry Point

The criminal acquires credentials and PII via methods such as:

- Purchasing credentials on the dark web
- Social engineering
- Locating open source info on the web
- Running a phishing scam
- Leveraging malware that will record keystrokes on the target's computer
- Using a cracking tool for a manual brute attack

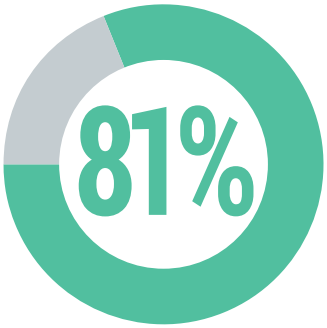


Automated Credential Stuffing Attacks

Buy, Trade, or Scrape Combolists

The criminal acquires credentials and tools for credential stuffing:

- Purchase or acquire an account checker tool that is valid for one or more sites
- Purchase, scrape, or otherwise obtain a combolist, which is a large list of usernames, emails, and passwords that can be loaded into account-checker tools
- Less commonly, an attacker might rent C2 / botnet infrastructure on the dark web, usually for a timeframe of 24-72 hours, and acquire an account stuffer and cracker to install on each bot (slightly more sophisticated because it costs money)



Of hacking-related breaches in 2020 ***leveraged weak or stolen passwords.***

- 2020 Verizon Data Breach Investigations Report

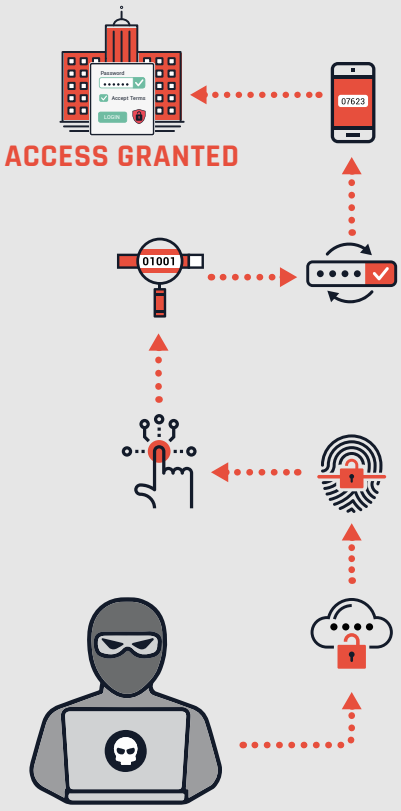
Stage 3: Obtain Access & Evade Detection

Targeted Account Takeover Attacks

Sophisticated and Varied Techniques

The criminal uses a variety of tactics, tools, and procedures to sidestep security measures and access accounts:

- Combining manual checks and specialized tools like purplespray to take a "low and slow" approach, systematically testing password variations without raising alarms
- Bypassing MFA via phishing, social engineering, man-in-the-middle attacks, iCloud vulnerabilities, or session hijacking
- Thwarting SMS-based 2FA with SIM-swapping, phone porting, or exploiting vulnerabilities in cell infrastructure (SS7 network)
- Pivoting tactics swiftly in response to new security measures



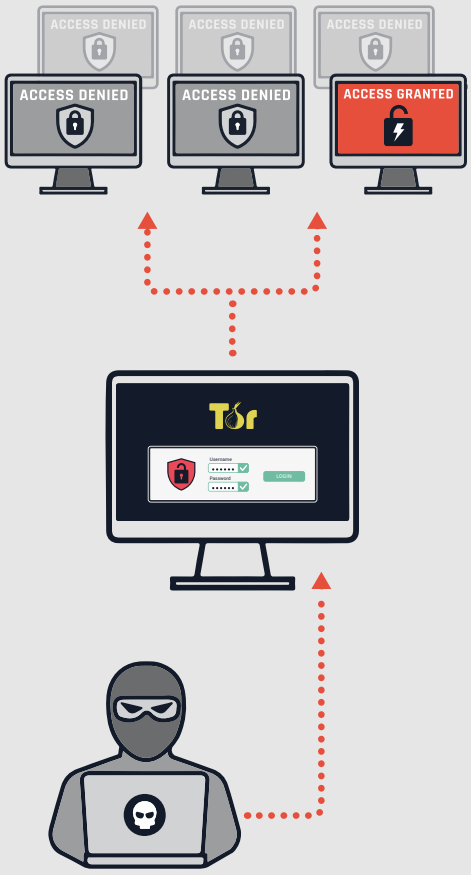
Automated Credential Stuffing Attacks

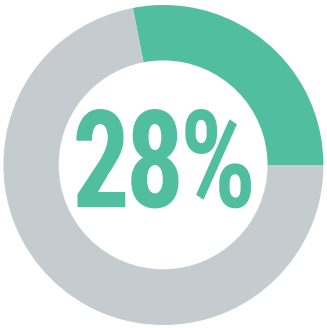
Unsophisticated, Uniform Tactics

The criminal uses their account checker tool to launch a credential stuffing attack against many accounts at one or more target organizations.

If using botnet infrastructure, they will issue commands from the C2 server to launch credential stuffing attacks at mass scale.

Because companies block malicious IP addresses, the attacker will use one or more methods of getting around IP blocking while using the account checker, such as free proxies, a VPN, and/or using TOR.





*Across 9 Billion credentials from 270 Million users, SpyCloud found that **28% of users recycled at least one password.***

- 2020 SpyCloud Credential Exposure Report

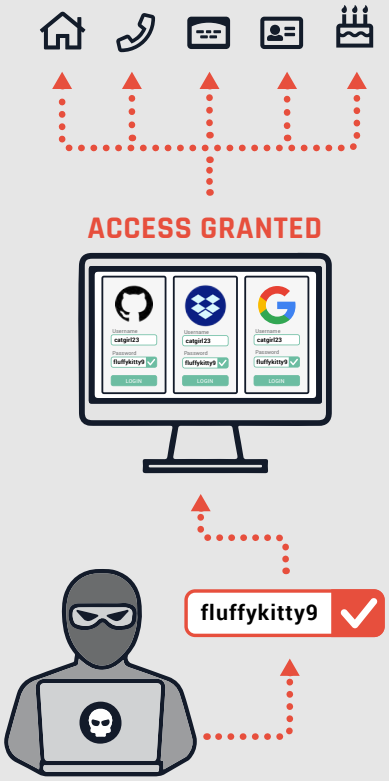
Stage 4: Escalate the Attack

Targeted Account Takeover Attacks

Escalation Is Common

Having gained access to an account, the criminal may escalate privileges or use one compromised account to reach additional targets. Tactics may include:

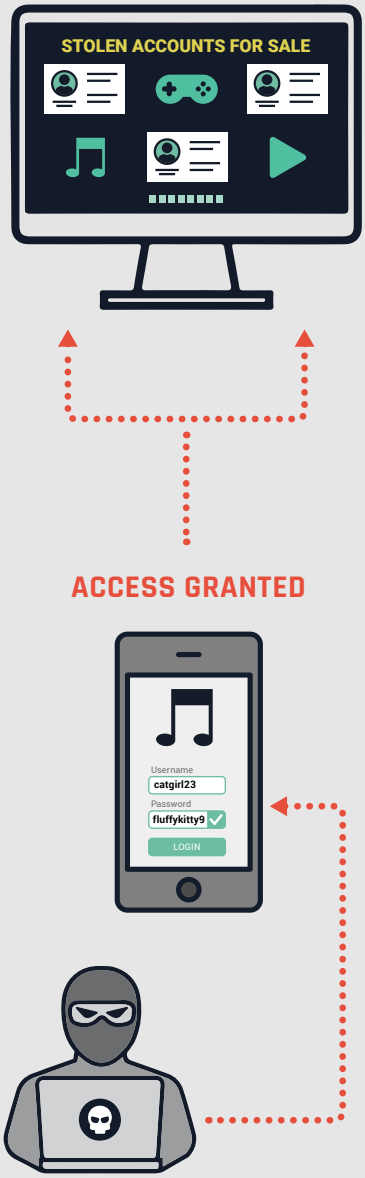
- Searching compromised email and storage accounts for TOTP seed backups or photos to use for authentication with other providers
- Cementing their ownership of an account by gradually changing contact info and other PII, locking the victim out of the account
- Using a victim's stolen account for targeted attacks against friends, coworkers, or clients
- Leveraging extortion, blackmail, and social engineering to gain additional access or control



Automated Credential Stuffing Attacks

Escalation Is Uncommon

Attack escalation is less common from criminals leveraging automated attacks, particularly because they intend to exploit the accounts themselves or resell them.



In targeted attacks, criminals use a variety of tactics, tools, and procedures to ***sidestep security measures and access accounts.***

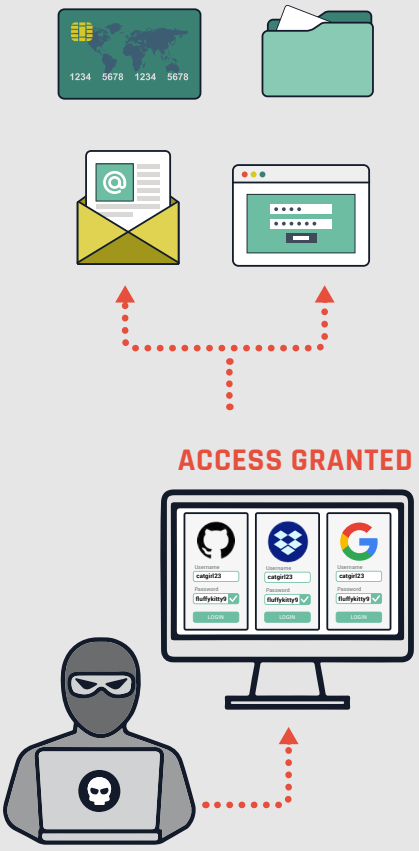
Stage 5: Exploit Stolen Accounts

Targeted Account Takeover Attacks

Achieve Targeted Objectives, Including High-Value Monetization

The criminal uses a variety of tactics, tools, and procedures to sidestep security measures and access accounts:

- Create new accounts
- Open credit cards
- Place fraudulent orders
- Gain access to victims' work accounts
- Conduct industrial espionage
- Wire or transfer money out of victims' accounts
- Sell account access to other criminals



Automated Credential Stuffing Attacks

Monetize Large Numbers of Low-Value Accounts

TWith access to stolen accounts, the criminal can:

- Sell account access to other criminals
- Place fraudulent orders using credit card information or gift cards stored within accounts
- Commit warranty fraud using stored device information
- Changing shipping addresses to facilitate package theft and drop-shipping
- Siphon loyalty points associated with the account

> *Without the SpyCloud data, we would be at constant risk for attacks we never saw coming*
>
> -Top Ten Travel Booking Site

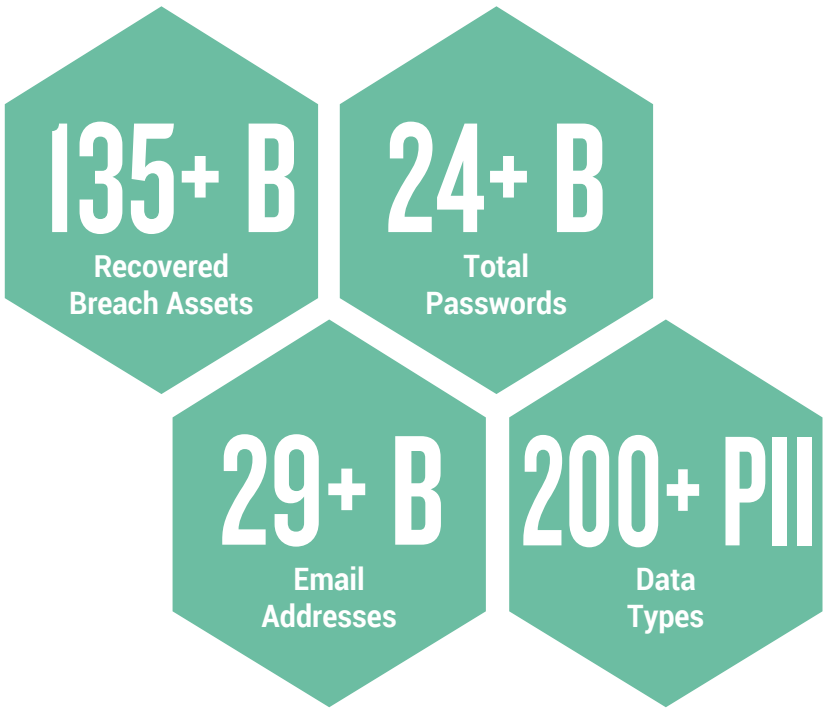
The SpyCloud Difference

Current, Relevant, Truly Actionable Data

Account takeover poses a substantial threat to enterprises and their customers. Unfortunately, all account takeover prevention solutions are not created equal. Many products, such as botnet firewalls and solutions that rely on commodity data, provide inadequate protection against the most damaging types of account takeover attacks. By gaining access to data early in the breach timeline, SpyCloud helps enterprises stay a step ahead of cybercriminals and protect against both targeted and automated account takeover attempts.

Using Human Intelligence, SpyCloud goes deeper into the web than any other cybersecurity company, extracting data that's otherwise undetectable. Our database of exposed credentials and PII is not only the largest in the industry—it offers the most current, relevant, and truly actionable data to protect users from account takeover.

Experience the power of our data for yourself. Visit spycloud.com to learn how SpyCloud can help your enterprise combat both targeted and manual account takeover attacks.



SpyCloud

Protect Your Users from Account Takeover with SpyCloud

Request a demo at spycloud.com