WHITEPAPER

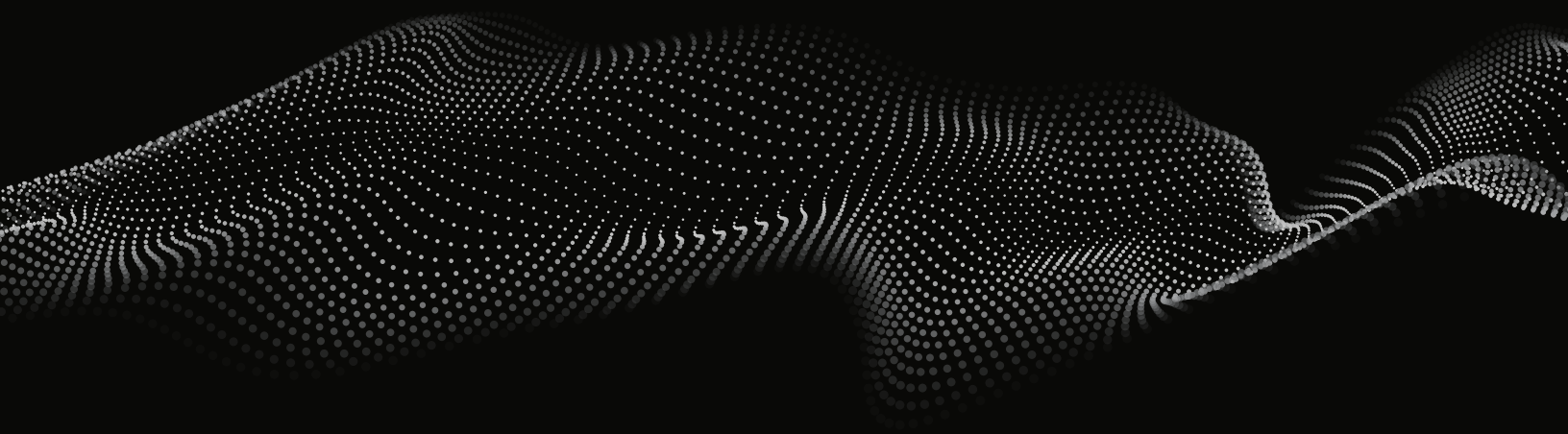
MFA Bypass 101

How Cybercriminals Combine Attack Methods and Stolen Credentials to Sidestep Multi-Factor Authentication

SpyCloud

SpyCloud

Table of Contents



SpyCloud

Introduction

In the wake of the 2020 SolarWinds attack, the US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) issued an advisory to organizations, warning that this was not a unique event. Highlighting an increasing number of attacks as more employees began to work remotely using corporate and personal devices during the COVID-19 pandemic, CISA noted several weaknesses in commonly used cybersecurity measures.

Of particular interest was mounting evidence that criminals had successfully bypassed multi-factor authentication (MFA) to compromise cloud service accounts.

As outlined in our 2022 Annual Identity Credential Exposure Report, SpyCloud observed a surge in infostealer (information-stealing malware) logs being distributed and shared on various forums and chat groups. Once devices are infected, keyboard strokes and system information is siphoned, exposing details ranging from login credentials and browser history to geolocation, installed software, autofill info, and even device and web session cookies. This information can be used to completely bypass authentication and fraud controls, including MFA.

A decade ago, MFA was heralded as a "magic bullet" that would make it much harder for criminals to break into an account. **Today, it's just another hurdle for determined hackers, who have developed an ever-growing list of ways to bypass it.**

What is MFA?

Any discussion of MFA must begin with passwords, which, despite their flaws, haven't diminished in popularity. Collectively, people have a habit of creating easy-to-guess passwords and re-using them across multiple accounts. To criminals, this is like leaving house keys in the lock on the front door – gaining access couldn't be easier.

Around a decade ago, security experts responded by encouraging organizations to embrace MFA. Designed as a security enhancement to the standard username/password combo, MFA required users to present two pieces of evidence before logging into an account.

Today, acceptable evidence, or "factors," generally amount to two of the following three categories:

- Something you know (a password, PIN, or passphrase)
- Something you have (a smartphone or physical token)
- Something you are (your fingerprint or face)

The obvious benefit of MFA is additional layers of protection. The idea is that more factors should make it harder for a potential intruder to gain access to accounts, systems or data. MFA can also help organizations achieve and maintain compliance, which can reduce liability concerns. But like all cybersecurity measures, it has its shortcomings.

- **Adoption is generally low**
  According to LastPass' 3rd Annual State of the Password Security Report, only 57% of businesses globally are using MFA and it varies greatly by country. Even among those who know better, MFA can be one hurdle too many for some users. That's because in most MFA implementations, passwords are still necessary. So now in addition to having to manage the password, users have to manage the additional layer of security.

- **Some users will accept any MFA request**
  Sometimes criminals don't even need to socially engineer someone into helping them. Here at SpyCloud, we heard from members of our Customer Advisory Board that some obliging customers will accept any MFA request, even if they're not currently trying to log into anything.

Stolen Credentials Are Fuel for Bypassing MFA

According to Microsoft's research, accounts are "more than 99.9% less likely to be compromised if you use MFA."

But this doesn't take into consideration the impact of already-stolen credentials, which are widely available on criminals marketplaces and forums, and were involved in nearly 80% of breaches last year.

To give you an idea of what's available to criminals, in our recent Identity Exposure Report, **security researchers at SpyCloud analyzed more than 1.7 billion credential pairs recaptured from data breaches and malware-infected device logs**. When looking to bypass MFA on their way to ATO, these credentials are of high value to criminals for a few reasons:

- Rampant password reuse means if a criminal has login info for one of your accounts, they can assume you use the same password (or a close variation) for other accounts.

- So much of our PII is shared willingly on social media that criminals can use it to guess answers to common MFA security questions (place of birth, high school mascot, etc.).

- Access to stolen phone numbers makes it easy for SIM-swapping to occur, where criminals intercept MFA codes sent via text message.

MFA Bypass Methods

If any good came out of the SolarWinds attack, it's that it raised awareness of how easily, frequently, and cleverly criminals get around MFA, not to mention how damaging a single successful bypass can be. While these attacks can take on many technical methods or combinations of methods, it's safe to assume that **attackers already have the victim's password.**

Session Hijacking

Session hijacking is a method criminals use to take over a user's web session without the need to authenticate via login credentials or MFA. When a user successfully logs into a web application (with one factor, two factors or ten factors), the server sets a temporary session cookie in the browser. This allows the remote server to remember that you're logged in and authenticated. Cybercriminals steal session cookies in a variety of ways, including:

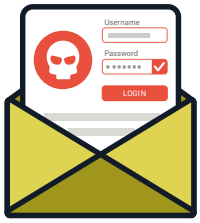
- Information-stealing malware
- Man-in-the-middle (MiTM) attacks
- Tricking the user into clicking a malicious link that contains a prepared session ID

With the stolen cookie, the attacker can take control of the session in their own browser – the server is fooled into thinking that the attacker's connection is the same as the real user's original session.

Once the attacker has hijacked the session, they can do anything that the original user is authorized to do. Depending on the targeted website, this can mean fraudulently purchasing items, accessing detailed personal information that can be used for identity theft, stealing confidential company data, or draining a bank account. Session hijacking can also be an easy way to launch a ransomware attack, as a criminal can hijack the session of a company VIP, and then access and encrypt valuable company data.

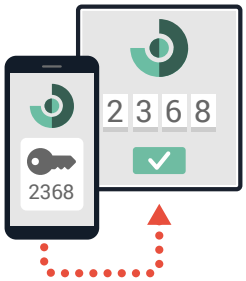
Forging Recognized Devices

Many times, an application will not require MFA from a device where users have logged in before. This is sometimes called adaptive multi-factor authentication (aMFA). In this case, attackers can try to figure out how the application recognizes a device and forge the signature of a recognized or "trusted device." For example, if a site marks recognized devices by using a predictable cookie, attackers can add that cookie value to their requests.



Phishing Emails

One of the oldest types of cyberattacks, phishing has evolved over the years but the goal remains the same – to trick an email recipient into believing that the message is something they want or need and to click a link or download an attachment. In MFA bypass attacks, these can involve technical support scams in which criminals convince users to install software that allows a "tech support expert" to log in remotely to solve their issue. In other phishing attacks, unsuspecting users are presented with a login experience that looks normal, but is actually a fake site that captures their authentication codes and user credentials.



Stealing One-Time Passwords

When MFA requires "something you own," it usually means your mobile device, hardware security key, or email account. These devices and accounts enable the use of one-time passwords (OTPs) as the secondary authentication factor, which are generated for a limited period and serve as an additional factor in the authentication process.

One method that gets around the use of OTP as a factor for authentication goes back to phishing. One such phishing scam begins when the victim lands on a spoofed website. The first step will be to steal their credentials ("what they know"), and then the scam will be initiated behind the scenes without the victim's knowledge. A direct authentication process against the targeted website or login portal using the stolen credentials will initiate a request for the OTP that will lead to a token being sent to the victim's device.

The victim is now connected to the phishing website and unaware that it is a scam. They will willingly provide their OTP token to the phishing website, which gives the scammers the ability to take over their account.

SIM Swapping

Despite education advising otherwise, many services still offer SMS text messaging for MFA. At this point, criminals have figured out ways to infiltrate cellular carrier networks, where with knowledge of the victim's cell phone company, they can easily perpetrate SIM swapping attacks.

In a SIM swapping attack, typically the attacker calls the phone companies' customer service department and finds someone who is willing to provide information to complete the SIM swap. Once the attacker has control over the customer's phone number, they call the bank to request a wire transfer from the victim's accounts to another account they own. The bank, recognizing the phone number as belonging to the customer, does not ask for full security questions but instead requests a one-time code sent to the phone number from which the attacker is calling.

In 2019, the FBI specifically issued a warning about SIM swapping since they've seen a steady increase in complaints regarding customers of US banking institutions targeted by cyber attackers who port the customer's phone number to a phone owned by the attacker.

Answering Security Questions

If you've ever had to have your MFA reset or turned off temporarily because you've gotten a new phone, for example, personally identifiable information (PII) is often used to prove that you are who you say you are. But PII is constantly exposed in data breaches, and we also give it away on social media — your pet's name, the last time you bought a car, how many kids you have, etc. All manner of data is out there and has been exposed either willingly or via breaches and it doesn't take much for a criminal to connect the dots and use our PII to circumvent MFA.

Preventative Measures

Think about account security like a home alarm. With a home alarm system, we place sensors on the doors and windows in an effort to slow intruders – but what happens when they don't trip those sensors? The motion detectors are the failsafe.

MFA is a great first step, but if a user logs in with valid credentials (aka account takeover), the organization has no way to determine if the user is a criminal because they trip no sensor. Although it's clear that attackers can circumvent MFA through social engineering and technical attacks, that doesn't mean you shouldn't use it. Any implementation of MFA should be predicated on the fact that it can be penetrated and does require additional considerations. Among them:

- ✓ **Monitor Credentials and Cookies for Compromise**
  It only takes one errant click, stolen credential, or stolen session cookie for the bad guys to break in and take over an account. The ability to know which of your users' credentials or cookies have been exposed is critical to mitigating the risk of breaches and fraud.

- ✓ **Implement Risk-Based Authentication**
  Think of risk-based authentication (RBA) like MFA on steroids. Similar in concept, RBA goes beyond the username/password and MFA code to include factors that uniquely identify the point-of-login, such as device profile, geolocation, and time of day. Risk-based policies, like prompting for a step-up authentication challenge when trying to access resources through an unauthorized proxy or automatically blocking access from known malicious IPs, can also kick in when triggered by suspicious events.

- ✓ **Install Antivirus and Anti-Malware Software**
  With more than 25 million new types of malware registered since the beginning of 2022 alone, there is no better time to step up your malware protection and overall cybersecurity than now. Trusted antivirus software could help protect your devices against malware attacks threatening your organization and valuable information.

- ✓ **Educate Users**
  It is critical to be aware that some MFA technologies are not fully protecting users from scams that compromise their accounts. This is bad news for individuals, but it can have severe consequences for organizations. All it takes is one employee to accept an illegitimate MFA push and the attacker has full account access. And with more individuals working remotely and potentially accessing professional tools and sites from personal devices, it's imperative that employees understand the risk of these infiltrations and that organizations have mitigation efforts in place to combat.

We recommend bolstering your cybersecurity program with credential exposure monitoring so you are alerted when accounts are compromised very early in the breach lifecycle (before criminals can exploit them for all the forms of MFA bypass mentioned above), along with automated remediation of those exposed credentials (making it less of a burden for you to keep your users safe).

Ultimately, there is no one "magic bullet" for cybersecurity. Implementing NIST guidelines, which include MFA operating in parallel with continuous monitoring for exposed credentials, allows organizations to easily pivot if fraud trends change or a new threat emerges.

SpyCloud

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 recaptured credentials and PII, is an important layer of defense for cyber attacks that leverage stolen data. We enable enterprises to detect and automatically reset compromised passwords early and invalidate compromised web sessions, negating the value of breached data before criminals have a chance to use it.

Our customers continue to tell us their ability to prevent account takeover, ransomware, and online fraud hinges both on access to relevant data and in being able to make that data operationally actionable through automation.

See Your Company's Risk

Discover how much data SpyCloud has recaptured for your domain. Once you know, you can take action.

Learn More

Enterprise Protection

Prevent account takeover that can lead to ransomware.

Learn More

Consumer Protection

Combat account takeover and online fraud.

Learn More

Investigations

Unmask criminals attempting to harm your business.

Learn More

Data Partnerships

Enhance your solution with SpyCloud's data.

Learn More

SpyCloud