INSIDE THE CRIMINAL MINDSET:

Sidestepping Authentication in a Passwordless World

SpyCloud

CONTENTS

INTRODUCTION

Passwords have been a cornerstone of security for centuries. From Shakespeare's "Long Live the King" in Hamlet to "Open Sesame!" in Ali Baba and the Forty Thieves, the concept of a passphrase to grant access is deeply rooted in our culture. Despite the plethora of accounts and services we use today, passwords remain a primary security measure. However – for the first time in history – we're starting to see this change.

The digital security landscape is shifting from passwords and password managers towards passwordless authentication, with passkeys beginning to take over traditional passwords. Passkeys promise a more streamlined and secure user experience, eliminating many of the age-old challenges associated with password management.

But if we've learned anything from the past, it's that cybercriminals are pretty good at adapting to change. As we move toward a passwordless digital society, adversaries are finding new avenues to exploit – including session hijacking – and challenging even the most sophisticated authentication systems.

This whitepaper breaks down modern authentication practices and provides guidelines on how to properly defend against next-generation authentication bypass or sidestepping techniques.

THE CURRENT STATE OF AUTHENTICATION

The current state of authentication is a blend of traditional methods and emerging technologies, each with its own set of advantages and challenges.

PASSWORDS

Despite their vulnerabilities, passwords remain the most common form of authentication. They are easy to implement and familiar to users. However, the human element introduces several challenges, such as password reuse, weak passwords, and phishing attacks. SpyCloud's **2023 Identity Exposure Report** found that 72% of breached passwords are still in use, and 61% of consumers repeat passwords across multiple accounts.

PASSWORD MANAGERS

Considering these statistics, the natural next step for many organizations is to use a password manager. Password managers reduce risk by generating strong passwords and storing them in a secure vault behind a single "master" password. But, while password managers make life more difficult for adversaries, they're not bulletproof. For one, the master password is user-generated, leading to the same risks with even greater consequences by exposing the entire vault. SpyCloud researchers uncovered nearly **118,000 stolen master passwords** from 8 password management providers, suggesting that password managers – while beneficial – cannot mask poor password hygiene.

MULTI-FACTOR AUTHENTICATION

Recognizing the limitations of password-only authentication, many organizations have adopted multi-factor authentication (MFA). This authentication method requires users to provide two or more verification factors to gain access. Common forms of MFA include something you know (password), something you have (a smart card or token), and something you are (biometrics). MFA enhances security by ensuring that even if one factor is compromised, an attacker still needs to bypass the other factors.

But MFA adoption remains **low**. And like all other cybersecurity measures, it's not infallible. Criminals can still use phishing, infostealer malware, and other techniques to intercept the authentication factors and perpetrate **account takeover**.

As bad actors evolve alongside authentication methods, we are now seeing organizations move toward passwordless authentication, as it offers some substantial advantages.

PASSKEYS: THE NEW ERA OF PASSWORDLESS AUTHENTICATION

As passwords are phased out, passkeys offer a simplified and secure method for users to sign in without the need for passwords. This technology leverages biometric authentication data (like fingerprints or facial scans) or PINs to authenticate users accessing supported websites and applications – presenting a more user-friendly alternative to traditional passwords while simultaneously enhancing security.

Fundamentally, a passkey is a cryptographic entity that remains invisible to the user and serves as a replacement for a password. It consists of two keys: a public key registered with the website or application, and a private key stored on the user's device(s).

This new authentication method has been gaining traction, especially since the **FIDO Alliance** began promoting the rollout of passkeys. Major tech giants, including Microsoft, Google, and Apple, have since launched the necessary infrastructure to support this new system.

Some of the benefits of passkeys include:

- They are associated exclusively with the website or application for which they were created, safeguarding users from potential phishing attempts.
- Passkeys can be stored in the cloud, making them accessible across multiple devices.
- The private key never leaves the user's devices, preventing potential leaks from websites or applications.
- Users don't need to create, protect, or remember anything about the passkey.

NOT USING PASSKEYS YET?

Not all organizations have transitioned to passwordless authentication. If passwords are used to secure your systems and accounts, consider implementing the following password guidelines, as recommended by NIST:

DO:

- Require a minimum length of 8 characters
- Allow 64+ character passwords
- Limit failed login attempts
- Ban passwords that are commonly used, expected, or previously compromised

DON'T:

- Require password complexity
- Force arbitrary password changes
- Use password hints or reminders
- Use knowledge-based authentication

BUT BEWARE OF THE HIDDEN DANGERS OF PASSWORDLESS AUTHENTICATION.

WHILE PASSKEYS ARE A TREMENDOUS IMPROVEMENT OVER PASSWORDS, CYBERCRIMINALS ARE SIMPLY WORKING AROUND PASSWORDLESS AUTHENTICATION WITH SESSION HIJACKING ATTACKS.

SIDESTEPPING AUTHENTICATION WITH SESSION HIJACKING

WHAT IS SESSION HIJACKING?

Whether a session was originally authenticated with a password or a passkey, every site and application assigns a cookie – a string of characters that the site or server uses to remember visitors and make it easier to visit the site again without authenticating. Some cookies may last only 24-48 hours, while others last for months or even years.

Session hijacking is an emerging, hard-to-detect attack method that grants a bad actor access to an already-authenticated session. Armed with an anti-detect browser and a valid cookie exfiltrated from an infostealer-infected device, an attacker can mimic a trusted device and ***sidestep all forms of authentication*** – passwords, MFA, and passkeys. We see supporting evidence of this rising attack method in the SpyCloud database, which included **22 billion** recaptured stolen cookie records from the darknet in 2022 alone.

THE CONSEQUENCES OF SESSION HIJACKING

Session hijacking is an increasingly prevalent way criminals are perpetrating fraud that's extremely difficult to detect. Think of it as next-generation account takeover – a way to mimic legitimate users without setting off red flags, which creates opportunities to escalate privileges and deliver executables. And yet the SpyCloud **2023 Ransomware Defense Report** found that security practitioners rated stolen cookies/tokens as a low-risk entry point for ransomware, which implies a lack of understanding of the scope of the session hijacking problem.

The exposure a stolen session cookie creates for the user and organization goes far beyond the initial malware infection. Once the cookie data is available on the criminal underground, it can be sold and traded several times to perpetrate different attacks by criminals of all skill levels as long as it remains valid. And if the stolen cookie links to an ongoing single sign-on (SSO) session, it could grant an attacker access to hundreds of applications in a **typical large enterprise**, making follow-on attacks overwhelmingly easy.

HOW TO PREVENT SESSION HIJACKING

As passwordless authentication continues to evolve, it remains a worthwhile component of a layered zero trust security approach and a big improvement over traditional password usage. That being said, additional strategies, such as monitoring for compromised web sessions and invalidating stolen session cookies are essential to prevent session hijacking.

For organizations to thwart attacks, it takes early insight into malware-compromised sessions and the ability to quickly invalidate the cookies and reset the credentials of infected users – before the stolen access data can be used. SpyCloud research shows that even when organizations have visibility into stolen session cookies, **39% of them still don’t terminate session cookies** at the sign of exposure.

To proactively prevent next-generation authentication bypass or authentication sidestepping, consider these steps:

STEP 1

ENFORCE **TIME-BOUND** SESSIONS

The longer a session remains active, the more time a potential attacker has to hijack it. By limiting your cookies’ time-to-live, even if an attacker gains access, their window to cause harm is significantly reduced. For critical applications, consider setting sessions to expire after shorter durations – for some applications, this might be minutes of inactivity, while for others, the time-to-live could be multiple days or weeks. It’s a balance between potential risk and your users’ tolerance for re-authenticating.

STEP 2

IMPLEMENT **CONTINUOUS** MONITORING

Deploy monitoring tools that deliver insights into malware-infected users and compromised cookies so you know exactly which web sessions to invalidate.

In addition, monitor for user behavior anomalies with tools that alert you of deviations from the norm, such as accessing the system from an unfamiliar IP address or performing high-volume data transfers. Integrating machine learning can further enhance the system's ability to detect anomalies by learning from historical data.

STEP 3

EDUCATE AND TRAIN

EARLY INSIGHTS into malware-compromised sessions can help organizations act quickly to prevent session hijacking – and maintain the integrity of your passwordless authentication solution.

THE KEY IS TO:

- Identify users infected by infostealers
- Invalidate any active sessions identified by a compromised cookie
- Reset exposed credentials
- Flag user accounts with known compromised devices for increased scrutiny of future logins or site interactions, regardless of cookie expiration time

The introduction of new technologies, especially those related to security, often requires a shift in mindset and behavior. Passwordless authentication, while offering numerous advantages, is not complete protection from infostealer malware infections. As with all things security, complementing technology solutions with human behavior training is vital to prevent next-generation attacks like session hijacking.

PREPARING FOR A PASSWORDLESS TOMORROW

Authentication is at a pivotal juncture. The transition from passwords to passkeys and beyond offers a glimpse into a more secure digital future. Yet it also serves as a reminder of the constant need for vigilance, education, and – particularly – adaptation in the face of evolving threats such as session hijacking.

As we transition into this new era, our approach to digital security must be holistic, accounting for the human element, but also adapting our technological defenses wherever possible to keep ahead of next-generation attack methods.

ABOUT SPYCLOUD

SpyCloud transforms recaptured darknet data to protect businesses from cyberattacks. Its products operationalize Cybercrime Analytics (C2A) to produce actionable insights that allow enterprises to proactively prevent ransomware and account takeover, safeguard employee and consumer identities, and investigate cybercrime incidents. Its unique data from breaches, malware-infected devices, and other underground sources also powers many popular dark web monitoring and identity theft protection offerings. SpyCloud customers include half of the ten largest global enterprises, mid-size companies, and government agencies around the world. Headquartered in Austin, TX, SpyCloud is home to nearly 200 cybersecurity experts whose mission is to make the internet safer with automated solutions that help organizations combat cybercrime.

To learn more and see insights on your company's exposed data, visit **spycloud.com**.