BLACKSWAN CYBERSECURITY

THREAT ADVISORY
Passkey Authentication Compromise (Pass-the-Passkey)
September 8, 2026

Severity: High
Threat Category: Identity Compromise, Authentication Bypass, Credential Enrollment Abuse
Affected Technologies:

- FIDO2/WebAuthn implementations
- synchronized passkeys,
- Windows passkey authentication,
- browser credential stores,
- password managers,
- account recovery systems, and
- passkey enrollment workflows.

Executive Summary

Security researchers have documented at least **39 attack methods, exploitation scenarios, and research techniques** that can compromise accounts protected by passkeys. These techniques generally do not extract a hardware-protected private key or defeat the underlying public-key cryptography. Instead, they manipulate authentication requests, capture or replay signed assertions, abuse synchronized credential stores, register attacker-controlled passkeys, exploit recovery processes, or operate from an already-compromised endpoint.

The attacks demonstrate an important distinction:
A passkey can remain cryptographically secure while the account, endpoint, authentication ceremony, session, or recovery process is compromised.

> For example, malware running on a Windows endpoint may invoke the legitimate WebAuthn infrastructure and cause Windows to display an apparently valid authentication prompt. If the user completes verification, the operating system generates a legitimate signed assertion that the malicious application may capture or redirect. The private key does not leave its protected storage, but the attacker still obtains usable authentication material.

Other documented research targets synchronized passkeys. Palo Alto Networks Unit 42 demonstrated attacks against Google's synchronized passkey environment in which malware on a compromised Windows endpoint could abuse onboarding, recovery, and device-trust workflows, bypass user-verification requirements, or recover synchronized passkey private keys.

Organizations should not abandon passkeys. FIDO2/WebAuthn still eliminates or significantly reduces many attacks based on password theft, password reuse, credential stuffing, and conventional credential phishing. However, passkey deployment must be treated as an **identity lifecycle and endpoint-security program**, not simply as a replacement authentication factor.

BLACKSWAN CYBERSECURITY

THREAT ADVISORY
Passkey Authentication Compromise (Pass-the-Passkey)

September 8, 2026

Threat Overview

Primary attack surfaces

The documented attack methods target one or more of the following trust boundaries:

1. Endpoint operating system
2. Browser and WebAuthn implementation
3. Authentication prompt and user interface
4. Signed WebAuthn assertions
5. Cloud-synchronized passkey vaults
6. Password-manager exports and credential exchange
7. Passkey registration and enrollment
8. Account recovery and temporary access mechanisms
9. Help desk and identity-verification processes
10. Cross-device and Bluetooth-assisted authentication
11. Authenticated browser sessions and tokens
12. The user approving the authentication request

A passkey ceremony may involve the application, browser, operating system, authenticator, password manager, synchronization provider, mobile device, Bluetooth transport, account-recovery system, enrollment process, help desk, and end user. Compromise of one sufficiently trusted component can allow an attacker to bypass the protection expected from the credential.

Technical Details

Passkey assertion capture and replay

A WebAuthn authenticator signs a relying-party challenge after required user-presence or user-verification checks. The resulting assertion is returned to the application for validation.

SpecterOps Pass-the-Passkey documented attacks involving:

- Passkey assertion mining from Windows event logs
- Assertion replay
- Assertion phishing
- Challenge injection
- Browser and WebAuthn hooking
- Assertion capture
- Detour attacks
- Passkey-to-token attacks
- User-presence and user-verification manipulation

THREAT ADVISORY
Passkey Authentication Compromise (Pass-the-Passkey)
September 8, 2026

CVE-2026-34348 concerned a Windows Event Logging Service issue associated with WebAuthn assertion exposure. Reporting indicates that Microsoft's July 2026 Windows updates made assertions written to affected event logs unusable for the demonstrated replay chain. Microsoft also stated that it applied mitigations for the separately reported passkey relay-assertion issue.

This specific chain should therefore be treated as **patch-addressable**, while assertion interception, malicious invocation, endpoint compromise, and implementation weaknesses remain part of the broader threat model.

Legitimate prompt abuse

Malware does not always need to counterfeit the Windows authentication dialog. It may invoke legitimate authentication functionality and cause the operating system to display a real prompt. Research tooling can repeatedly invoke passkey prompts, obtain the resulting assertion after user verification, enumerate available Windows Hello credentials, and monitor WebAuthn-related events.

The user may believe the prompt belongs to a trusted browser or application when the ceremony was initiated by malicious code.

Applicable techniques include:

- Passkey prompt flooding
- Application metadata spoofing
- Credential-interface deception
- Credential UI overlay
- Window-handle spoofing
- Remote Desktop passkey phishing
- FIDO interface overlays

This recreates a risk historically associated with MFA push fatigue: users may approve a legitimate-looking request that they did not initiate.

Synced-passkey compromise

Synchronized passkeys expand the security boundary from one authenticator to the systems that store, synchronize, restore, and recover the credential.

Documented targets include:

- Google or Apple cloud-account takeover
- Compromised password-manager accounts
- Stolen cloud synchronization secrets

- Malicious browser extensions
- Compromised or rooted mobile devices
- Infostealer malware
- Passkey vault export files
- KeePassXC and Bitwarden exports
- Credential exchange or migration files
- Cloud recovery and new-device enrollment

Unit 42 Pass the Passkey: A Novel Attack Surface in Passwordless Authentication describes attack classes against Google's synchronized passkey ecosystem. Starting from malware executing on a compromised endpoint, the research demonstrated abuse of onboarding and recovery workflows, authentication without expected user interaction, bypass of user-verification requirements, and extraction of synchronized private keys.

Shadow passkeys and unauthorized enrollment

An attacker may avoid stealing the legitimate passkey entirely. After compromising an account, recovery channel, endpoint, help-desk interaction, or temporary credential, the attacker can attempt to register a new passkey under the attacker's control.

Relevant attack scenarios include:

- Shadow passkey registration
- Attacker-controlled phone enrollment
- Enrollment vishing
- Help-desk impersonation
- Temporary access credential abuse
- SIM-based recovery
- Reverse-vishing attacks
- Device-migration pretexts
- Unauthorized authenticator replacement

The newly registered credential is legitimate from the service's perspective. Consequently, weak recovery or enrollment controls can undermine otherwise strong authentication.

Post-authentication session theft

Passkeys protect the authentication ceremony, not necessarily the entire authenticated session. Malware, adversary-in-the-middle infrastructure, browser compromise, or session-token theft may allow an attacker to hijack a session after the legitimate user completes passkey authentication.

THREAT ADVISORY
Passkey Authentication Compromise (Pass-the-Passkey)
September 8, 2026

This means that successful passkey authentication should not be treated as permanent proof that all subsequent activity originates from the verified user. Sensitive transactions may require continuous risk evaluation, transaction-specific authorization, or renewed authentication.

Threat Actor Tactics, Techniques, and Procedures

The following MITRE ATT&CK mappings are an **analyst assessment** based on the behavior described in the cited research. The exact mapping will depend on the attack implementation.

ATT&CK ID	Technique	Application to Passkey Compromise
T1189	Drive-by Compromise	Delivery of malicious browser content or code that compromises the endpoint used for passkey authentication.
T1204.001	User Execution: Malicious Link	User follows a link leading to a malicious application, enrollment flow, or authentication prompt.
T1204.002	User Execution: Malicious File	Malware is installed on the endpoint that hosts or accesses passkeys.
T1056	Input Capture	Hooking or monitoring authentication interfaces and collecting authentication outputs.
T1056.002	GUI Input Capture	Credential-interface overlays and deceptive authentication windows.
T1111	Multi-Factor Authentication Interception	Capturing or redirecting authentication assertions or user-approved authentication results.
T1539	Steal Web Session Cookie	Theft of the authenticated session created after passkey authentication.
T1550.004	Use Alternate Authentication Material: Web Session Cookie	Reuse of a stolen token or cookie without repeating the passkey ceremony.
T1555.003	Credentials from Web Browsers	Access to browser credential stores, passkey-related material, or synchronized vault information.
T1555.005	Password Managers	Theft or abuse of passkeys and exports maintained by password managers.
T1546	Event Triggered Execution	Hooking browser or authentication processes to capture authentication events.
T1036	Masquerading	Spoofed application metadata or displays that make a prompt appear associated with a trusted application.
T1021.001	Remote Services: Remote Desktop Protocol	Remote Desktop passkey phishing or authentication-prompt manipulation.
T1078	Valid Accounts	Use of an attacker-enrolled shadow passkey or a compromised synchronized credential.
T1098	Account Manipulation	Addition of a passkey, authenticator, recovery method, device, or other persistence mechanism.
T1098.005	Account Manipulation: Device Registration	Registration of an attacker-controlled device through abused enrollment or recovery workflows.
T1566	Phishing	Vishing, reverse vishing, recovery pretexts, and deceptive enrollment instructions.
T1484	Domain or Tenant Policy Modification	Potential modification of identity or authentication policies after privileged compromise.

THREAT ADVISORY
Passkey Authentication Compromise (Pass-the-Passkey)
September 8, 2026

Representative attack chain

1. Attacker delivers malware or obtains code execution on a user endpoint.
2. Malware enumerates browser, Windows Hello, or synchronized passkey capabilities.
3. The attacker invokes or intercepts a WebAuthn request.
4. A legitimate or deceptive prompt is displayed.
5. The user verifies or approves the request.
6. Malware receives, captures, or redirects the signed assertion.
7. The attacker exchanges the assertion for a session or authentication token.
8. The attacker establishes persistence by registering a new passkey or recovery method.
9. The attacker uses the valid account for data access, privilege escalation, lateral movement, fraud, or business email compromise.

Indicators of Compromise

IOC availability

The research describes **attack methods rather than one malware family or campaign**. Therefore, there is no universal set of malicious hashes, domains, IP addresses, filenames, or certificates applicable to all passkey-compromise activity.

Organizations should focus on **behavioral indicators and identity telemetry**.

Identity and enrollment indicators

- New passkey or authenticator registration without a corresponding approved request
- Passkey enrollment from an unmanaged or previously unseen device
- Multiple passkey registrations shortly after account recovery
- Addition of a passkey following a help-desk reset or temporary access credential
- New device registration followed by access to sensitive applications
- Changes to phone numbers, recovery email addresses, or recovery methods
- Removal of a legitimate authenticator after enrollment of a new one
- Authentication-method changes performed outside established support workflows
- High-value users switching from an enterprise-controlled authenticator to a synchronized consumer passkey
- Passkey registration from an unusual IP address, autonomous system, geography, or browser profile

Authentication indicators

- Repeated passkey prompts not associated with a user-initiated sign-in
- Successful passkey authentication followed immediately by access from a different IP address or device

- Authentication assertion received without the expected browser session context
- Unexpected changes in authenticator class or attachment type
- Abnormal user-verification or user-presence results
- Identical or suspiciously similar assertion material presented more than once
- Authentication attempts containing malformed, substituted, or mismatched challenges
- Unexpected cross-device or hybrid authentication activity
- Passkey authentication followed by immediate OAuth consent, mailbox-rule creation, or privilege change

Endpoint indicators

- Untrusted processes invoking WebAuthn or Windows credential-interface APIs
- Non-browser processes generating passkey authentication prompts
- Repeated WebAuthn calls from scripting engines, unsigned binaries, or newly installed applications
- Process injection or API hooking involving browsers or authentication components
- Access to password-manager databases or credential export files
- Browser extensions installed outside the approved enterprise catalog
- Memory-access activity directed at browsers or credential-management processes
- Infostealer detections, cookie theft, DPAPI access, or browser-profile collection
- Unexpected access to Windows WebAuthn event data
- Remote Desktop sessions immediately preceding passkey prompts
- A passkey prompt whose displayed application does not correspond to the foreground process

Post-compromise indicators

- Concurrent sessions from inconsistent devices or locations
- Session-token use without a corresponding recent authentication event
- Creation of persistence through OAuth applications, inbox rules, delegated permissions, or recovery changes
- Download or access activity inconsistent with the user's normal role
- Privileged operations immediately after passkey enrollment
- Rapid access to multiple SSO-connected applications
- Attempts to disable identity alerts, EDR controls, or authentication logging

Recommendations

Priority 1: Immediate actions

1. **Patch Windows endpoints promptly.** Confirm deployment of updates addressing CVE-2026-34348 and subsequent WebAuthn, browser, and identity-platform security updates.

Reporting indicates that Microsoft's July 2026 Windows updates disrupted the demonstrated Windows event-log replay chain.

2. **Investigate every endpoint with infostealer or credential-theft activity.** Passkey use does not neutralize malware already executing in the user's session. Treat browser-memory access, password-manager access, session-token theft, and suspicious WebAuthn invocation as potential identity compromise.
3. **Inventory registered passkeys.** Identify user, device, authenticator type, enrollment date, synchronization capability, and whether the credential is enterprise-managed.
4. **Review recent enrollment and recovery events.** Prioritize privileged users, executives, administrators, help-desk personnel, finance staff, and users with access to sensitive or regulated data.
5. **Revoke sessions after suspected compromise.** Removing the attacker's passkey alone may not invalidate session cookies, refresh tokens, application passwords, OAuth grants, or registered devices.

Priority 2: Harden enrollment and recovery

- Require an existing strong authenticator to authorize new passkey enrollment.
- Require step-up verification for authenticator replacement.
- Prohibit help-desk personnel from registering passkeys on behalf of users.
- Require documented identity verification and supervisory approval for high-risk resets.
- Send out-of-band notifications for new passkeys, device registrations, and recovery-method changes.
- Place a delay or heightened monitoring period on sensitive actions following account recovery.
- Restrict temporary access credentials by lifetime, scope, device, and permitted enrollment activity.
- Remove weak SMS, email, and knowledge-based recovery paths where feasible.
- Develop a specific response playbook for unauthorized passkey enrollment.

The FIDO Alliance Passkeys: The Journey to Prevent Phishing Attacks emphasizes that phishing resistance requires strengthening both authentication and account-recovery processes, rather than treating deployment as a single technology change.

Priority 3: Protect high-value identities

For privileged and high-impact accounts:

- Prefer enterprise-managed, device-bound, or hardware-backed authenticators.
- Evaluate restrictions on synchronized or exportable passkeys.
- Limit enrollment to approved authenticator classes.

- Require managed and compliant endpoints.
- Require fresh authentication for privileged and destructive actions.
- Use separate administrative accounts and privileged access workstations.
- Apply just-in-time privilege elevation.
- Prevent weaker authentication methods from silently functioning as fallback paths.

Dedicated hardware reduces exposure to cloud synchronization, password-manager export, malicious mobile applications, and consumer account-recovery paths, but it must be combined with correct relying-party configuration and secure enrollment.

Priority 4: Endpoint and browser controls

- Deploy EDR/XDR coverage to all devices capable of performing passkey authentication.
- Use application control to restrict unsigned or unapproved executables.
- Prevent unauthorized browser extensions.
- Monitor processes invoking WebAuthn and credential APIs.
- Harden remote access and Remote Desktop use.
- Isolate endpoints with infostealer or session-theft indicators.
- Restrict local administrator privileges.
- Monitor browser and credential-process memory access.
- Protect password-manager exports and prohibit unapproved credential migration.
- Maintain browser, operating-system, password-manager, and authenticator firmware updates.

Priority 5: Session and application protections

- Use short-lived sessions appropriate to application risk.
- Reevaluate risk during an authenticated session rather than relying only on the initial passkey event.
- Require fresh authentication for payment changes, administrative actions, credential changes, and sensitive exports.
- Bind sessions or tokens to devices where the application and identity platform support it.
- Reject authentication challenges that are expired, previously used, malformed, or not bound to the expected transaction.
- Validate origin, relying-party identifier, challenge, authenticator data, signature, user-verification state, and expected session context.
- Monitor token reuse and impossible or implausible session transitions.
- Terminate all sessions when a passkey, recovery method, or registered device is determined to be malicious.

THREAT ADVISORY
Passkey Authentication Compromise (Pass-the-Passkey)
September 8, 2026

Priority 6: User and help-desk awareness

Users should be instructed to:

- Approve a passkey request only when they personally initiated the sign-in.
- Cancel and report unexpected authentication or enrollment prompts.
- Never enroll a new passkey at the direction of an unsolicited caller.
- Never share screens or grant remote control during identity recovery unless following a verified internal process.
- Report repeated passkey prompts as a potential security event.
- Verify the application, website, and action before completing biometric or PIN verification.

Help-desk personnel should be trained specifically on passkey enrollment vishing, shadow passkeys, SIM-based recovery abuse, temporary credential misuse, and executive impersonation.

Incident Response Guidance

If passkey compromise is suspected:

1. Disable or contain the affected identity based on business impact.
2. Isolate the endpoint used during suspicious authentications.
3. Revoke active sessions, refresh tokens, and remembered browser sessions.
4. Remove unauthorized passkeys, devices, recovery methods, and OAuth grants.
5. Preserve identity-provider, endpoint, browser, EDR, help-desk, and enrollment logs.
6. Determine whether the event involved assertion abuse, synchronized-key exposure, shadow enrollment, session theft, or account recovery.
7. Hunt for identical enrollment, prompt, and device-registration activity across other accounts.
8. Reset affected cloud-synchronization or password-manager credentials where applicable.
9. Reestablish access through a verified clean device and approved authenticator.
10. Monitor the identity for renewed registration, token use, privilege changes, or abnormal application access.

If a synchronized private key may have been extracted, simple password rotation is insufficient. The affected passkey should be removed and replaced, the credential-sync environment investigated, active sessions revoked, and the endpoint rebuilt or remediated according to the organization’s incident-response standard.

Risk Assessment

Overall Risk: High

Likelihood: Medium to High for targeted organizations, especially where users authenticate from unmanaged endpoints or use synchronized consumer passkeys.

THREAT ADVISORY
Passkey Authentication Compromise (Pass-the-Passkey)
September 8, 2026

Impact: High to Critical for privileged, executive, financial, help-desk, cloud-administration, and identity-management accounts.

Key risk amplifiers:

- Weak passkey enrollment controls
- SMS or email recovery fallback
- Unmanaged devices
- Consumer synchronization services
- Unrestricted password-manager exports
- Excessive local privileges
- Limited endpoint monitoring
- Long-lived sessions
- Weak help-desk identity verification
- Lack of alerts for authenticator and device changes

Partnering with Blackswan to Strengthen Identity Security

Blackswan Cybersecurity helps organizations reduce identity-based risk through a combination of advisory services and managed security operations. Our team can assess passkey readiness, identity architecture, enrollment and recovery procedures, Microsoft 365 security controls, and Zero Trust maturity to identify weaknesses before attackers do. Through our **Managed Security Services (MSSP)** and **24x7 XDR/SOC monitoring**, we help detect suspicious authentication activity, unauthorized device registrations, account takeover attempts, session hijacking indicators, and identity-based attack techniques. Our recommended technology stack includes **Huntress Managed EDR** for endpoint detection and response, **Huntress Managed Identity Threat Detection and Response (ITDR)** capabilities, **IRONSCALES Email Security** to reduce phishing and social engineering risk, and integrated SIEM/XDR monitoring to correlate identity, endpoint, and email security events. In addition, Blackswan provides incident response readiness, tabletop exercises, threat hunting, compromise assessments, and rapid-response services to help organizations identify, contain, and recover from modern identity-centric attacks before they disrupt business.

For more information, contact Blackswan Cybersecurity to schedule an Identity Security and Passkey Readiness Assessment.