

INTELLIGENCE BRIEF

OAuth Data Theft Can Survive a Password Reset

The FBI's September consent-phishing warning and the earlier Drift breach expose two routes to SaaS data theft. Review app permissions, revoke unauthorized grants, and investigate the data already accessed.

EDITION

Fall/Winter 2026/2027 Edition

BA-02 · Breach analysis

PUBLISHED BY

Z7 Solutions LLC

Orlando, Florida

READ ONLINE

z7solutions.com

844-974-8669

01 At a Glance

STATUS

ONGOING RISK

November 3 review of dated consent-phishing and integration-theft evidence.

HEADLINE NUMBERS

2
Access paths separated in this brief

Sep 1
2026 FBI consent-phishing warning [1]

KEY FACTS

RECENT WARNING
FBI consent-phishing PSA, September 1, 2026 [1]

HISTORICAL INCIDENT
Drift-associated Salesforce data theft, August 2025 [2]

CONSENT ROUTE
A malicious app receives user-approved permissions [1]

INTEGRATION ROUTE
Previously trusted OAuth tokens are compromised [2]

INVESTIGATION SCOPE
Granted permissions, connected systems, accessed records [2]

RESPONSE OWNERSHIP
Application administrators and incident responders [3]

02 What Happened

September 2026 FBI guidance and the August 2025 Drift breach illustrate distinct SaaS access risks, reviewed here November 3. [1, 2]

- The FBI describes deceptive messages leading to a legitimate consent screen, where a malicious app receives permissions without obtaining the user's password. [1]
- Google tracked Drift-token misuse against Salesforce during August 8 through August 18, 2025, without a core Salesforce vulnerability. [2]
- Google expanded the affected integration scope on August 28, 2025. That historical update is not evidence of a fresh November incident. [2]

- Cloudflare's September 2, 2025 disclosure describes stolen Salesforce support-case text and a response that re-established integrations with new secrets. That experience shows why incident scope includes information copied into support conversations. [5]

03 How It Works

01 Win a grant or steal a token

Consent phishing wins new app permissions. Integration theft takes existing service credentials. Triage them as separate hypotheses. [1, 2]

02 Exercise the granted permissions

Access follows the app's permissions and the compromised connection. Microsoft administrators can review both user and administrator consent records. [3]

03 Read and export business records

In the Drift campaign, Google observed data exports and searches for credentials inside the stolen material. A support record can therefore become a route to another environment. [2]

04 Leave access after the reset

The FBI warns that password changes do not remove the malicious grant. Responders must address app authority separately. [1]

04 Who Is at Risk

The FBI warning and the Drift incident involve different victim populations. Their shared lesson applies wherever a cloud app can read valuable records.

- Prominent people and their contacts targeted by deceptive messages. [1]
- Businesses with customer data reachable through SaaS integrations. [2]
- Teams that paste credentials or sensitive configuration details into support cases. [5]

Sectors in scope: Organizations using email, file-sharing and CRM SaaS, Executives and other prominent individuals, Support and sales teams with third-party integrations.

05 What Changed Since the Last Edition

EACH CHANGE WITH ITS SOURCE

01 September 1, 2026: the FBI published a warning about consent phishing observed since late 2025. This is the recent advisory driving this review.

SOURCE 1

02 August 2025: Google expanded the historical Drift advisory beyond Salesforce integration exposure.

SOURCE 2

03 Current Microsoft administration guidance distinguishes tenant-wide administrator consent from per-user grants and explains their different revocation methods.

SOURCE 3

06 What to Do Now

IN PRIORITY ORDER, HIGHEST IMPACT FIRST

01 DO FIRST **Restrict user consent and establish a reviewed approval route.**
Microsoft documents policy controls for user consent; evaluate the permissions and business need before approving an app. [4]

02 **Inventory app grants with an owner and a business purpose.**
Review both user-consented and administrator-consented permissions, including grants that exceed what the application needs. [3]

03 **Revoke unauthorized grants using the supported method.**
Microsoft notes that per-user grants cannot be revoked through the administrator portal's User consent tab; use its documented Graph or PowerShell path with an authorized administrator. [3]

04 **Contain the compromised integration and rotate relevant secrets.**
Cloudflare disconnected and securely re-established integrations during its response; coordinate changes with service owners to preserve necessary business workflows. [5]

05 **Investigate the records and systems the connection could reach.**
Google recommends examining connected systems; preserve relevant logs and scope credential exposure in exported records. [2]

06 Confirm containment before calling the incident closed.

Z7 recommends an authorized access check and follow-up log review to verify the unwanted app authority has ended. [3]

07 Indicators

Indicators the sources publish, as they print them. Hunt with them, and check the source before you block.

BEHAVIOR — Unfamiliar integration access, unusually large data exports, or logins from unfamiliar locations. [5]

BEHAVIOR — Unexpected application permissions discovered during a user-consent or administrator-consent review. [3]

08 Sources

[1] **Malicious Cyber Actors Gain Access to Victim Accounts Through Consent Phishing** FBI Internet Crime Complaint Center · September 1, 2026. https://www.ic3.gov/PSA/2026/PSA260901

[2] **Widespread Data Theft Targets Salesforce Instances via Salesloft Drift** Google Threat Intelligence Group · August 26, 2025; updated August 28, 2025. https://cloud.google.com/blog/topics/threat-intelligence/data-theft-salesforce-instances-via-salesloft-drift

[3] **Review permissions granted to enterprise applications** Microsoft · Updated March 6, 2025; reviewed November 3, 2026. https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/manage-application-permissions

[4] **Configure how users consent to applications** Microsoft · Updated June 24, 2025; reviewed November 3, 2026. https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/configure-user-consent

[5] **The impact of the Salesloft Drift breach on Cloudflare and our customers** Cloudflare · September 2, 2025. https://blog.cloudflare.com/response-to-salesloft-drift-incident/

NEXT STEP

What does this mean for your security?

Bring your questions about OAuth grants and integration tokens, your environment and the controls you rely on. Talk through the most useful next step with Z7 Solutions LLC.

01 / Exposure

Bring one question about how this threat could affect your environment.

02 / Priorities

Bring your current safeguards, open gaps and budget questions.

ALSO IN THIS EDITION

SitusAMC breach settlement and vendor risk
More from the edition · z7solutions.com/z7-cyber/situs/

Qilin still tops most ransomware counts
More from the edition · z7solutions.com/z7-cyber/qilin/

Qilin still hits hospitals and infrastructure
More from the edition · z7solutions.com/z7-cyber/qilin-part-2/

CALL 844-974-8669

EMAIL sales@z7solutions.com

BOOK A SECURITY CONVERSATION Book a Security Conversation ↗

Z7 Solutions™, Z7-Claw™ and Z7-Guard™ are trademarks of Z7 Solutions LLC.