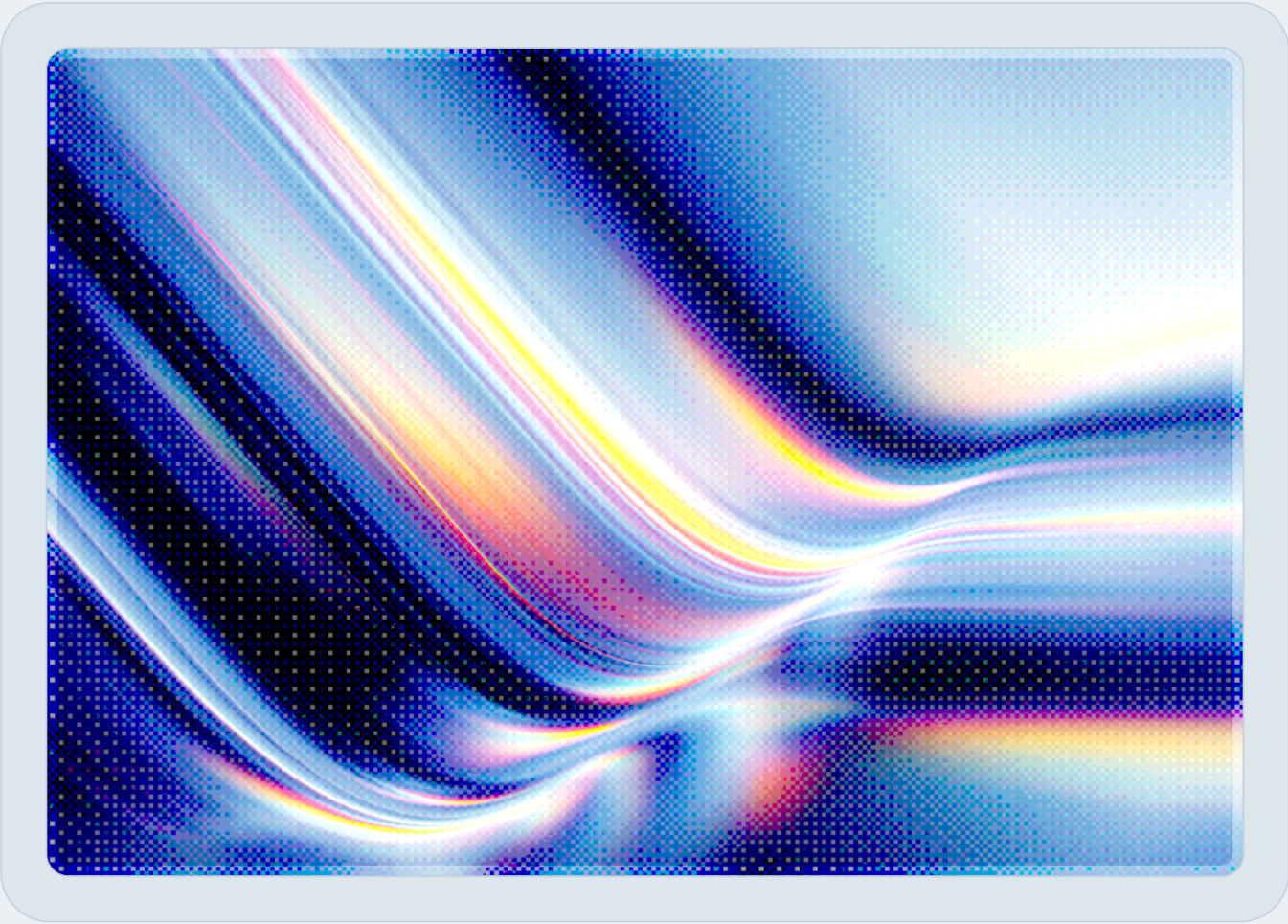
CSAI Foundation | Cloud Security Alliance

ShinyHunters' OAuth Pivot: A Year of SaaS Supply-Chain Breaches

Salesloft, Gainsight, and Klue Expose the Third-Party OAuth Trust Gap

2026-07-16

AI-assisted Rapid Research



CSAI | CSA cloud security alliance®

Key Takeaways

- Between August 2025 and June 2026, actors operating under the ShinyHunters brand — now folded into a broader collective some researchers track as Scattered Lapsus$ Hunters — ran three successive OAuth-token supply-chain compromises against Salesloft's Drift integration, Gainsight's published Salesforce applications, and the Klue competitive-intelligence platform, reaching customer Salesforce data without exploiting any Salesforce platform vulnerability [1][2][11].
- Confirmed exposure scales differ sharply by incident: Salesloft/Drift affected more than 700 organizations, including Cloudflare, Zscaler, and Palo Alto Networks [4][5]; the Gainsight compromise reached more than 200 Salesforce instances [7]; and Klue confirmed to customers that OAuth tokens tied to 195 organizations were affected, including cybersecurity vendors Huntress and Recorded Future [9][10][19].
- The common root cause across all three incidents was durable, overlooked OAuth trust rather than end-user credential phishing: a four-year-old dormant test credential at Klue, a GitHub-to-AWS pivot into Salesloft's token store, and reuse of Salesloft-derived tokens to gain a foothold in Gainsight's published apps [1][8][10].
- Standard Salesforce authentication and sign-in monitoring did not flag any of the three incidents because the malicious queries arrived through already-authorized connected-app sessions rather than new logins — a detection blind spot Microsoft and Salesforce have only recently begun closing with connected-app risk scoring and OAuth scope visibility tooling [1][2].
- The campaign reads as a deliberate pivot: the same actor set spent mid-2025 voice-phishing employees into directly authorizing rogue Salesforce "Data Loader" apps, then shifted to the higher-leverage strategy of compromising vendors that already held legitimate OAuth grants across hundreds of customers simultaneously [1][3].

Background

Salesforce environments are an attractive target for financially motivated extortion actors: a single connected application can hold read access to an organization's most complete store of customer and prospect data, and that access, once granted, is typically trusted indefinitely — a dynamic this note's three incidents illustrate directly. The campaign now associated with ShinyHunters did not begin with the OAuth-token thefts that are the focus of this note; it began with voice phishing. Starting in mid-2025, callers impersonating internal IT support convinced Salesforce administrators and end users to authorize a malicious connected application disguised as Salesforce's own Data Loader tool. Google's own Salesforce instance was compromised this way in June 2025, with the company later confirming that attackers obtained "largely public business contact data" and that the intrusion was part of the same UNC6040 activity affecting other organizations [1][16].

On August 8, 2025, a Telegram channel appeared claiming to unite the membership and branding of Scattered Spider, Lapsus$, and ShinyHunters under a single banner, a grouping researchers have since labeled Scattered Lapsus$ Hunters [11][12]. Within days, the group's tradecraft shifted from phishing individual victims to compromising the vendors that already held legitimate OAuth grants into those victims' Salesforce instances — a shift that, whether or not deliberate, multiplied the reach of a single compromise from one organization to hundreds [4][5]. Between August 8 and 18, 2025, the intrusion cluster Google tracks as UNC6395 used OAuth and refresh tokens stolen from Salesloft's Drift AI chat integration to query and export data from Salesforce environments belonging to more than 700 organizations, including Cloudflare, Palo Alto Networks, Proofpoint, PagerDuty, and Tanium [4][5]. The root cause traced back further still: investigators found that attackers had accessed Salesloft's GitHub account as early as March 2025, using that foothold to compromise Salesloft's AWS environment and harvest the OAuth secrets later used against customer Salesforce orgs [1][5]. Salesloft and Salesforce jointly revoked all active Drift tokens on August 20, 2025, and Salesforce pulled Drift from its AppExchange pending investigation [4]. Separately, other organizations linked to the wider UNC6040/UNC6240 vishing wave that summer included Chanel, Pandora, Adidas, Qantas, Allianz Life, and several LVMH properties [16][17][18].

The pattern repeated in November 2025, when Salesforce detected unusual API activity associated with applications published by Gainsight, a customer-success platform, and disabled the Gainsight-published apps across its ecosystem. GTIG linked the intrusion to ShinyHunters-affiliated actors and assessed that the campaign reached more than 200 Salesforce instances, with some reporting indicating the attackers leveraged OAuth tokens carried over from the earlier Salesloft compromise to establish persistent API access [2][7]. A third wave followed in June 2026. Klue, a competitive-intelligence SaaS vendor, had created a credential years earlier to prototype an integration it subsequently abandoned without deactivating; on June 11, 2026, attackers authenticated using that four-year-old dormant credential,

pushed a code update capable of harvesting customer OAuth tokens, and ran automated scripts against the Salesforce REST API for roughly 24 hours before Klue detected the intrusion on June 12 [8][9]. The breach reached OAuth tokens for 195 Klue customer organizations, exposing Salesforce data at cybersecurity vendors Huntress and Recorded Future, among others [9][10][19]. A group calling itself Icarus — identified through session-messenger IDs in extortion emails that matched a dark-web leak site — claimed responsibility, and Microsoft separately tracks the actor behind the Klue intrusion as Storm-3138 [2][10].

Security Analysis

OAuth as the Durable Perimeter

Each of the three incidents exploited the same structural property of OAuth-based SaaS integration: once a connected application is authorized, it typically retains access indefinitely, independent of the human session that granted it. A compromised OAuth or refresh token lets an attacker query an API on a schedule and at a volume that would trigger alerts if attempted through a browser login, yet the same activity through an approved integration would typically produce API traffic that is difficult to distinguish from the vendor's legitimate service calls. Salesforce's own authentication logs, built to flag anomalous user sign-ins, were not designed to evaluate what an already-trusted connected application does once inside the environment, which helps explain why none of the three intrusions were caught through login monitoring [1][2]. The attackers understood this asymmetry: in the Klue incident, the automated harvesting ran for roughly a day before discovery, and in the Salesloft case the exfiltration window stretched across more than a week [4][9].

Three Incidents, One Weak Link

Although the three compromises targeted different vendors, they share a common failure mode: a durable OAuth credential that nobody was actively reviewing. The following comparison highlights the structural similarities and differences across the campaign.

Incident	Compromise Window	Entry Point	Confirmed Scale	Attribution
Salesloft Drift	Aug 8–18, 2025	GitHub access (Mar 2025) → AWS pivot →	700+ organizations [4][5]	UNC6395 (Google)

Incident	Compromise Window	Entry Point	Confirmed Scale	Attribution
		stolen OAuth/refresh tokens		
Gainsight	Nov 2025	Anomalous API activity via Gainsight-published apps; possible reuse of Salesloft-derived tokens	200+ Salesforce instances [7]	ShinyHunters-affiliated (GTIG)
Klue	Jun 11–12, 2026	Four-year-old dormant test credential → OAuth token harvesting	195 customer organizations [9][10][19]	Icarus / Storm-3138 (Microsoft)

The table understates one important continuity: in each case, the compromised vendor was a trusted third party whose own security posture — not Salesforce's — determined whether customer data stayed protected. Salesforce's shared-responsibility model places OAuth scope discipline, connected-app review, and vendor credential hygiene on the customer and the integration vendor, but these integrations are commonly treated with far less scrutiny than a privileged administrative account would receive. CSA's 2025–2026 State of SaaS Security survey of 420 security professionals found that 58% of organizations struggle to enforce least-privilege access across their SaaS integrations and 46% lack adequate visibility into non-human identities such as OAuth-connected applications, survey findings consistent with the gap this campaign's three incidents illustrate [1][6][20].

An Evolving and Contested Attribution Picture

Attribution across this campaign is genuinely unsettled, and readers should weigh confidence levels accordingly. Google's tracking separates the mid-2025 vishing wave (UNC6040/UNC6240) from the Salesloft token-theft cluster (UNC6395) [16][4], and its ongoing analysis of the broader campaign has introduced still further designations — UNC6661 and UNC6671 — for later-identified activity clusters [3]. Later Gainsight and Klue activity is attributed to "ShinyHunters-affiliated" actors and, in Klue's case, to a specifically named group (Icarus) that Microsoft maps to its own designation, Storm-3138 [2][10]. ShinyHunters itself has publicly claimed that the cumulative campaign reached close to 1,000 organizations, a figure that industry researchers have not independently confirmed and that should be treated as an extortion narrative rather than a verified count [2]. The August 2025 emergence of a

Telegram channel uniting Scattered Spider, Lapsus$, and ShinyHunters branding further complicates attribution, since the same infrastructure and monikers may now be used by overlapping or loosely affiliated actors rather than a single command structure [11][12].

Recommendations

Immediate Actions

Security teams should inventory every OAuth-connected application authorized against their Salesforce and adjacent SaaS environments, with particular attention to integrations from Salesloft (Drift), Gainsight, and Klue, and confirm whether any of those integrations were active during the disclosed compromise windows. Any organization that used the Drift, Gainsight, or Klue integrations during their respective incident windows should treat associated OAuth and refresh tokens as compromised, revoke and reissue them, and review exported data logs for evidence of bulk queries consistent with the reported tradecraft. Teams should also specifically search their connected-app inventory for credentials tied to abandoned pilots, proof-of-concept integrations, or deprecated tools — the exact category of dormant access that enabled the Klue compromise — since these are the entries least likely to appear in a routine access review.

Short-Term Mitigations

Organizations should enable enhanced Salesforce event monitoring and connect their instances to a cloud access security broker or equivalent tooling capable of attributing API activity to specific connected applications rather than only to user sessions; Microsoft's recent Defender for Cloud Apps updates specifically target this gap [1]. Connected-app permissions should be scoped to the minimum required for each integration's function, with read and write access separated wherever the vendor supports it, and session or token lifetimes should be shortened for any application that does not require persistent access.

Strategic Considerations

Third-party OAuth grants should be governed with the same rigor organizations apply to privileged human accounts: a defined owner, a documented business justification, a scheduled re-certification date, and automatic revocation when an integration is decommissioned rather than left dormant. This lifecycle discipline would likely have surfaced and remediated the Klue credential, which instead remained live and unreviewed for four years. As agentic AI tools increasingly request their own OAuth grants into

CRM, ticketing, and collaboration platforms, organizations should extend this same third-party risk management discipline to AI agent integrations now, before this attack pattern extends to agent-issued OAuth tokens, as the same structural gap would apply.

CSA Resource Alignment

CSA's analysis of the Salesloft Drift incident is directly applicable to this broader campaign. The CSA blog post "The Salesloft Drift OAuth Supply-Chain Attack: Cross-Industry Lessons in Third-Party Access Visibility" examined the same intrusion cluster covered in this note and identified excessive permission scope, the absence of periodic OAuth lifecycle reviews, and blind spots in monitoring delegated access as the root governance failures, consistent with this note's analysis of the subsequent Gainsight and Klue incidents [6]. That post's recommendation to treat third-party connected applications "like privileged accounts" is the same discipline this note recommends applying to dormant and pilot integrations specifically.

The SaaS Security Capability Framework (SSCF) provides the technical control baseline that, if adopted by SaaS vendors and enforced by their customers, would have constrained each incident in this campaign. SSCF's Identity and Access Management domain — the framework's largest, with 21 of its 36 total controls — calls for separate read and write OAuth scopes, programmatic visibility into connected-app permissions, and session revocation capabilities, all of which map directly to the gaps exploited at Salesloft, Gainsight, and Klue [13]. Organizations conducting third-party risk assessments of SaaS vendors with Salesforce access should use SSCF's control specifications as an evaluation checklist rather than relying solely on general compliance attestations like SOC 2.

CSA's 2025–2026 State of SaaS Security survey provides the empirical baseline underlying this campaign's shared root cause, documenting the least-privilege enforcement gaps and non-human identity visibility gaps described above across a sample of 420 security professionals — evidence that the OAuth trust failures at Salesloft, Gainsight, and Klue reflect a widespread industry condition rather than three isolated lapses [20]. CSA's presentation "Take a Deep Dive Into Common SaaS Data Breaches — And How to Avoid Them" analyzes prior real-world SaaS breach scenarios built around OAuth token abuse and third-party application compromise, and its central recommendation — that organizations gain visibility into what authorized integrations actually do with their access, rather than trusting the initial authorization decision indefinitely — is directly relevant to all three incidents in this note [14]. Finally, the AI Controls Matrix (AICM) v1.1 offers the broader governance frame for organizations formalizing third-party and non-human identity risk management: its control domains covering supply chain and vendor risk provide a structure for documenting which integrations hold which scopes, a practice this note's immediate-actions guidance treats as foundational [15].

References

1. Microsoft Security Blog, "Defending SaaS-based applications against ShinyHunters' OAuth abuse," July 13, 2026.
2. The Hacker News, "Microsoft Maps Year-Long ShinyHunters Campaign Against SaaS Platforms," July 2026.
3. Google Cloud Blog, "Expansion of ShinyHunters' SaaS Data Theft Campaigns," Google Threat Intelligence Group, 2026.
4. Google Cloud Blog, "Widespread Data Theft Targets Salesforce Instances via Salesloft Drift," Google Threat Intelligence Group, August 2025.
5. The Hacker News, "Salesloft Takes Drift Offline After OAuth Token Theft Hits Hundreds of Organizations," September 2025.
6. Cloud Security Alliance, "The Salesloft Drift OAuth Supply-Chain Attack: Cross-Industry Lessons in Third-Party Access Visibility," September 25, 2025.
7. BankInfoSecurity, "ShinyHunters Hack Salesforce Instances Via Gainsight Apps," November 2025.
8. The Hacker News, "Salesforce Disables Klue App Integration After OAuth Token Abuse Exposes Customer Data," June 2026.
9. Huntress, "Cybercrime Breaches Klue: Salesforce Data Impacted for Many Victims, Including Huntress," 2026.
10. CSO Online, "Klue Breach Exposed Salesforce CRM Data Through Stolen OAuth Tokens," 2026.
11. Mitiga, "Scattered Lapsus$ Shiny Hunters Strikes Salesforce Again," 2025.
12. Push Security, "Analyzing "Scattered Lapsus$ Hunters" Breaches Since 2021," 2026.
13. Cloud Security Alliance, "SaaS Security Capability Framework (SSCF)," September 2025.
14. Cloud Security Alliance, "Take a Deep Dive Into Common SaaS Data Breaches – And How to Avoid Them," 2025.
15. Cloud Security Alliance, "AI Controls Matrix (AICM) v1.1," 2026.
16. Google Cloud Blog, "The Cost of a Call: From Voice Phishing to Data Extortion," Google Threat Intelligence Group, June 2025.
17. BleepingComputer, "ShinyHunters Behind Salesforce Data Theft Attacks at Qantas, Allianz Life, and LVMH," August 2025.

18. Infosecurity Magazine, "Chanel and Pandora Breached as Salesforce Campaign Continues," August 2025.
19. SecurityWeek, "More Klue Breach Victims Identified as Hackers Get Hacked," 2026.
20. Cloud Security Alliance, "The State of SaaS Security: 2025-2026," 2025.