INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-18 19:04 UTC

Salesforce Third-Party App Compromise Campaign Expands: Klue Battlecards Joins Growing Supply Chain Attack Series

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0514
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Salesforce (CRM platform, OAuth integration layer); Klue Battlecards (third-party Salesforce integration); additional unnamed third-party Salesforce-connected apps (at least 2 confirmed); affected customers including Huntress (cybersecurity vendor)
Published	2026-06-18T12:49:04
Discovery Source	Rss

Executive Summary

Attackers operating under the campaign name 'Icarus' are systematically compromising third-party applications connected to Salesforce via OAuth, then using that trusted access to extract CRM data from Salesforce customers. Klue Battlecards, a competitive intelligence tool used by sales and strategy teams, is the latest confirmed victim; its customers, including cybersecurity vendor Huntress, had Salesforce CRM data exposed. Any enterprise using third-party Salesforce-connected applications faces the same structural risk, as the attack targets the integration layer, not Salesforce itself.

Technical Analysis

The Icarus campaign exploits overprivileged OAuth token relationships maintained by third-party Salesforce integrations. Rather than attacking Salesforce's platform directly, adversaries compromise the third-party app (in this case, Klue Battlecards) and abuse its pre-authorized OAuth access to extract Salesforce CRM data. Relevant CWEs: CWE-732 (Incorrect Permission Assignment for Critical Resource), CWE-269 (Improper Privilege Management), and CWE-284 (Improper Access Control). MITRE ATT&CK techniques involved include T1528 (Steal Application Access Token), T1550.001 (Use Alternate Authentication Material: Application Access Token), T1078.004 (Valid Accounts: Cloud Accounts), T1530 (Data from Cloud Storage), T1195.002 (Supply Chain Compromise: Compromise Software Supply Chain), T1199 (Trusted Relationship), and T1567 (Exfiltration Over Web Service). No CVE has been assigned; the attack exploits architectural weaknesses in

OAuth scope management rather than a discrete software vulnerability. Klue Battlecards is the confirmed victim in this campaign series, with evidence of similar attacks on other third-party Salesforce integrations. No vendor patch is applicable; remediation is architectural: audit and revoke overprivileged OAuth tokens, enforce least-privilege scopes, and monitor connected app activity.

Action Checklist

1. Step 1: Containment. Log into Salesforce Setup > Connected Apps OAuth Usage and immediately revoke OAuth tokens for Klue Battlecards and any other third-party connected apps not actively required. Prioritize apps with broad object-level read scopes (Contacts, Opportunities, Accounts). Document which apps are revoked and notify affected business owners.
2. Step 2: Detection. Review Salesforce Event Monitoring logs (LoginEvent, ApiEvent, ConnectedApplicationEvent) for anomalous data access patterns originating from Klue or other third-party connected app OAuth sessions. Look for high-volume record reads, unusual access times, or API calls from unexpected IP ranges associated with third-party OAuth tokens. Cross-reference against NIST AU-6 audit review procedures.
3. Step 3: Eradication. Re-provision only required third-party OAuth connections using the principle of least privilege (NIST AC-6). Require Klue and any other affected vendor to confirm the breach vector is closed and provide evidence of credential rotation (D3-CRO) before re-authorizing. Enforce explicit scope restrictions on all reconnected apps.
4. Step 4: Recovery. After re-authorizing any required integrations, monitor Salesforce Event Monitoring for a minimum of 30 days for anomalous API activity. Validate that no unauthorized OAuth tokens remain active via Salesforce Setup > OAuth Connected Apps. Confirm with affected vendors they have completed their own incident investigation.
5. Step 5: Post-Incident. Conduct a full OAuth hygiene review across all Salesforce-connected applications, mapping each app's granted scopes against documented business need (aligned with NIST AC-3, AC-6, CIS 5.1). Establish a recurring quarterly review process for connected app permissions. Evaluate whether current third-party vendor due diligence processes include security posture assessments for OAuth integrations.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to legal, privacy counsel, and executive leadership immediately if Salesforce Event Monitoring logs confirm bulk export of Contact or Account objects containing PII — this triggers breach notification assessment under GDPR, CCPA, and applicable state laws, and if the affected organization is a Huntress-type cybersecurity vendor, customer notification obligations may be time-bound.

Recovery Notes	After revoking Klue and Icarus-campaign-linked OAuth tokens and re-provisioning with least-privilege scopes, maintain daily review of Salesforce ApiEvent RowsProcessed counts for all third-party connected apps for a minimum of 30 days to detect any residual attacker access via a token or integration not yet identified. Validate that no connected app added during the Icarus campaign window (check ConnectedApplicationEvent for new app authorizations in the 90 days preceding detection) remains active. Confirm with Klue and any other affected vendor that their own incident investigation is closed and that no Salesforce customer data extracted during the campaign is retained on attacker-controlled infrastructure before declaring the incident closed.
Forensic Artifacts	Salesforce ConnectedApplicationEvent logs filtered to Klue Battlecards OAuth client ID: captures the exact authorization grant timeline, associated Salesforce user, and session metadata for the Icarus campaign access window. | Salesforce ApiEvent logs with QueriedEntities and RowsProcessed fields: reveals which CRM object types (Contacts, Opportunities, Accounts) were bulk-read under the compromised Klue OAuth token and the volume of records exfiltrated per session. | Salesforce Setup > Connected Apps OAuth Usage export (timestamped CSV): the live token inventory at time of discovery — documents which apps held active tokens, their granted scopes, and last-used timestamps before revocation destroys this state. | LoginEvent records for the Salesforce integration user associated with the Klue OAuth grant: LoginType='OAuth 2.0', SourceIp, and LoginSubType fields identify whether attacker-controlled infrastructure relayed API calls through the compromised Klue token or accessed Salesforce directly. | Third-party vendor (Klue) incident attestation and credential rotation confirmation: documents the closure of the supply chain breach vector on the vendor side and serves as evidence that the re-authorized OAuth connection is not re-introducing the Icarus campaign access path.

Per-Action IR Details

Step 1: Containment — Log into Salesforce Setup > Connected Apps OAuth Usage and immediately revoke OAuth tokens for Klue Battlecards and any other third-party connected apps not actively required. Prioritize apps with broad object-level read scopes (Contacts, Opportunities, Accounts). Document which apps are revoked and notify affected business owners.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-12 (Session Termination), NIST AC-2 (Account Management), CIS 6.2 (Establish an Access Revoking Process)

Compensating: If you lack a dedicated Salesforce admin console workflow, use the Salesforce CLI (sf org list auth) to enumerate all authenticated OAuth sessions, then use sf org logout --target-org to revoke individual tokens. For a 2-person team: one analyst inventories connected apps via Setup > Connected Apps OAuth Usage export (CSV downloadable), while the second cross-references against an approved-app register. Document revocations in a shared Google Sheet or Confluence page timestamped to the minute.

Evidence: BEFORE revoking any OAuth token, export the full Salesforce Event Monitoring log snapshot covering the prior 90 days — specifically ConnectedApplicationEvent, ApiEvent, and LoginEvent records tied to Klue Battlecards and any other third-party OAuth client IDs. Capture the active token list (client ID, granted scopes, last-used timestamp, associated user) from Setup > Connected Apps OAuth Usage as a timestamped screenshot or CSV. This live token state is destroyed the moment revocation occurs and is your primary evidence of the blast radius — which Salesforce objects (Contacts, Opportunities, Accounts) were accessible under the compromised Klue OAuth grant.

Step 2: Detection — Review Salesforce Event Monitoring logs (LoginEvent, ApiEvent, ConnectedApplicationEvent) for anomalous data access patterns originating from Klue or other third-party connected app OAuth sessions. Look for high-volume record reads, unusual access times, or API calls from

unexpected IP ranges associated with third-party OAuth tokens. Cross-reference against NIST AU-6 audit review procedures.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), NIST AU-3 (Content Of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, query Salesforce Event Monitoring directly using SOQL via the Salesforce CLI: sfdx force:data:soql:query -q "SELECT CreatedDate, UserId, SourceIp, EventType, QueriedEntities, RowsProcessed FROM ApiEvent WHERE CreatedDate = LAST_N_DAYS:90 AND ConnectedAppName = 'Klue Battlecards'" -u . Export to CSV and load into a free tool such as VisiData or Google Sheets to pivot on RowsProcessed (flag any session returning >500 records in a single call) and SourceIp (flag non-Klue ASN ranges). Use OSINT (ipinfo.io free tier) to geolocate unexpected source IPs against Klue's known infrastructure.

Evidence: No live-state destruction occurs in this step — it is read-only analysis. Key artifacts to retrieve: (1) ConnectedApplicationEvent records filtered to Klue Battlecards OAuth client ID, showing EventDate, UserId, ConnectedAppName, and HttpMethod; (2) ApiEvent records showing QueriedEntities (look for bulk reads against Contact, Opportunity, Account objects), RowsProcessed, and SourceIp; (3) LoginEvent records for any service account or integration user associated with the Klue OAuth grant, capturing LoginType='OAuth 2.0', LoginSubType, and SourceIp. Flag API calls originating from IP ranges outside Klue's documented SaaS infrastructure as high-priority indicators of exfiltration relay or attacker-controlled infrastructure.

Step 3: Eradication — Re-provision only required third-party OAuth connections using the principle of least privilege (NIST AC-6). Require Klue and any other affected vendor to confirm the breach vector is closed and provide evidence of credential rotation (D3-CRO) before re-authorizing. Enforce explicit scope restrictions on all reconnected apps.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-6 (Least Privilege), NIST AC-3 (Access Enforcement), CIS 6.1 (Establish an Access Granting Process)

Compensating: For teams without an automated provisioning platform, enforce scope restriction manually by navigating to Salesforce Setup > Connected Apps > Edit for each re-provisioned app, and unchecking all object-level permissions not documented as required by the vendor. Require written attestation from Klue's security team (email or signed statement) confirming: (a) the OAuth client secret associated with the compromised integration has been rotated, (b) the breach entry point on Klue's side has been remediated, and (c) all active tokens issued under the old credential have been invalidated. Store this attestation in your incident record. Do not re-authorize any Klue or Icarus-campaign-linked app until this evidence is received.

Evidence: Before re-provisioning any OAuth connection, confirm that the prior revocation (Step 1) was complete by re-querying Setup > Connected Apps OAuth Usage for any residual active tokens under the old Klue client ID. Capture a final pre-re-provisioning snapshot of granted scopes for each app being re-enabled. If Klue provides a new OAuth client ID as part of their credential rotation, document both the old and new client IDs in your incident record — the old ID remains a forensic indicator for retrospective log analysis of the Icarus campaign activity.

Step 4: Recovery — After re-authorizing any required integrations, monitor Salesforce Event Monitoring for a minimum of 30 days for anomalous API activity. Validate that no unauthorized OAuth tokens remain active via Salesforce Setup > OAuth Connected Apps. Confirm with affected vendors they have completed their own incident investigation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-12 (Audit Record Generation), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without a SIEM for continuous monitoring, configure Salesforce's native Real-Time Event Monitoring (if licensed) or schedule a daily automated SOQL query via cron + Salesforce CLI that extracts ApiEvent and ConnectedApplicationEvent records for all re-authorized third-party apps and emails the RowsProcessed summary to the security team. Set a manual threshold alert: any single OAuth session returning >500 CRM records triggers immediate review. For the 30-day watch period, maintain a running log of daily record counts per connected app in a shared spreadsheet to enable trend analysis without a dedicated SIEM.

Evidence: No destructive action occurs in this step, but document the recovery baseline: export the current connected app list with granted scopes and last-used timestamps at the start of the 30-day watch period. This baseline is your comparison point for detecting any scope creep or new unauthorized apps introduced during the recovery window. Retain all Salesforce Event Monitoring logs from the incident window (pre-revocation through re-authorization) for a minimum of 12 months in immutable storage to support any regulatory breach notification obligations or downstream customer notification requests from Huntress-type customers affected by the Icarus campaign.

Step 5: Post-Incident — Conduct a full OAuth hygiene review across all Salesforce-connected applications, mapping each app's granted scopes against documented business need (aligned with NIST AC-3, AC-6, CIS 5.1). Establish a recurring quarterly review process for connected app permissions. Evaluate whether current third-party vendor due diligence processes include security posture assessments for OAuth integrations.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), NIST AC-20 (Use Of External Systems), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Build a no-cost OAuth inventory using a Salesforce SOQL query to enumerate all connected apps and their granted scopes: SELECT Name, MobileSessionTimeout, OptionsAllowAdminApprovedUsersOnly, OptionsRefreshTokenValidityMetric FROM ConnectedApplication. Export to CSV and map each app's scopes to a documented business justification column. For third-party vendor security posture assessment without a paid tool, require vendors to provide their most recent SOC 2 Type II report or equivalent attestation and verify Klue and similar competitive-intelligence tools are included in your vendor risk register. Schedule quarterly calendar reminders for the connected app review in whichever ticketing system (Jira, ServiceNow) the team uses.

Evidence: Produce a lessons-learned report documenting: (1) the full list of Salesforce objects exposed under the Klue Battlecards OAuth grant during the Icarus campaign window, (2) the total record count accessible under each compromised scope (drawn from ApiEvent RowsProcessed aggregates), and (3) any customers or business units whose Salesforce data was in scope. This report feeds both internal process improvement and any external breach notification obligations. Archive all Salesforce Event Monitoring exports, revocation timestamps, vendor attestations, and scope change records from this incident as a named evidence package for the Icarus campaign case file.

Detection Guidance

Primary detection surface is Salesforce Event Monitoring. Query ApiEvent and ConnectedApplicationEvent logs for: (1) high-volume record reads from OAuth sessions associated with Klue Battlecards or other third-party connected apps; (2) access to sensitive objects (Contacts, Opportunities, Leads, Accounts) outside normal business hours or at volumes inconsistent with integration baseline; (3) OAuth token usage from IP addresses not associated with the vendor's known infrastructure. In your SIEM, alert on Salesforce API calls exceeding normal per-session record thresholds for any connected app OAuth identity. Additionally, monitor for new OAuth app authorizations not initiated through your change management process (NIST AU-2, AU-6). Behavioral indicator: any third-party integration reading data across multiple CRM object types in a single session window warrants investigation. No public IOCs (IPs, domains, hashes) have been confirmed for this campaign at time of writing.

Framework Mappings

MITRE-ATTACK

- **T1530** — Data from Cloud Storage
- **T1195.002** — Compromise Software Supply Chain
- **T1078.004** — Cloud Accounts
- **T1567** — Exfiltration Over Web Service
- **T1199** — Trusted Relationship
- **T1550.001** — Application Access Token
- **T1528** — Steal Application Access Token
- **T1078** — Valid Accounts

NIST-800-53R5

- **CM-7** — Least Functionality
- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-3** — Access Enforcement
- **SR-2** — Supply Chain Risk Management Plan

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **3.3** — Configure Data Access Control Lists
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **15.1** — Establish and Maintain an Inventory of Service Providers

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC9.2** — Manages risks associated with vendors and business partners

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1530	Data from Cloud Storage	Collection
T1195.002	Compromise Software Supply Chain	Initial-Access
T1078.004	Cloud Accounts	Defense-Evasion
T1567	Exfiltration Over Web Service	Exfiltration
T1199	Trusted Relationship	Initial-Access
T1550.001	Application Access Token	Defense-Evasion
T1528	Steal Application Access Token	Credential-Access
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/cyberattacks-data-breaches/salesforce-d...	T3
Klue OAuth breach linked to 'Icarus' Salesforce data theft attacks	https://www.bleepingcomputer.com/news/security/klue-oauth-breach-li...	T3
Attackers Steal Salesforce Data From Klue Battlecards Users	https://www.govinfosecurity.com/attackers-steal-salesforce-data-fro...	T3
Win-Loss Battlecards Powered Klue's Salesforce Integration in Klue	https://klue.com/blog/win-loss-battlecards-salesforce	T3
Klue OAuth Breach Enabled Icarus Theft of Salesforce CRM Data	https://news.mallory.ai/stories/019edb44-57c2-756b-bec2-0cba596e0070	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-06-18 19:04 UTC by TJS Security Command Center