INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-18 19:03 UTC

Icarus Exploits Klue OAuth Chain to Exfiltrate Salesforce CRM Data Across Multiple Enterprises

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0512
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Klue Battlecards (OAuth integration layer), Salesforce CRM (REST API), HubSpot, SharePoint, Zoom, Gong, Chorus, Clari, Google Drive, Slack, all organizations using Klue's third-party integrations
Published	2026-06-18T10:19:50
Discovery Source	Rss

Executive Summary

Threat actor group Icarus compromised Klue's backend systems, harvesting OAuth tokens that granted access to Salesforce CRM environments across multiple enterprises. Attackers exfiltrated customer records, sales pipeline data, and enterprise contact information by querying Salesforce REST APIs using the stolen tokens, without directly breaching any customer environment. Affected organizations face active extortion; Salesforce has disabled the Klue Battlecards integration, and exposure across connected platforms including HubSpot, Gong, Slack, and SharePoint remains under investigation.

Technical Analysis

Icarus gained initial access to Klue's infrastructure via a dormant prototype credential, a hardcoded or residual account not decommissioned from development or staging environments (CWE-522: Insufficiently Protected Credentials, CWE-272: Least Privilege Violation). From that foothold, attackers injected malicious code into Klue's backend to harvest OAuth tokens stored within Klue's environment, exploiting insufficient session expiration controls (CWE-613) and improper authentication boundaries (CWE-287). The stolen tokens were used to authenticate directly against Salesforce REST APIs (T1528: Steal Application Access Token; T1078: Valid Accounts), bypassing Salesforce's own authentication layer because the tokens appeared legitimate. Data exfiltration occurred over web service channels (T1567) targeting cloud storage objects (T1530). The attack is classified as a software supply chain compromise (T1195.002), Klue's trusted OAuth integration status with Salesforce and other SaaS platforms was the pivot point. Icarus subsequently launched extortion campaigns against affected organizations (T1657). No CVE has been assigned. Salesforce has revoked the Klue

Battlecards integration. Potential exposure extends to HubSpot, SharePoint, Zoom, Gong, Chorus, Clari, Google Drive, and Slack through Klue's other OAuth integrations.

Action Checklist

1. Step 1: Containment. Immediately audit all active OAuth grants in Salesforce (Setup > Connected Apps OAuth Usage) and revoke any token issued to Klue Battlecards. If your organization uses HubSpot, Gong, Slack, Zoom, Chorus, Clari, Google Drive, or SharePoint via Klue integrations, revoke those OAuth grants as well. Salesforce has already disabled the Klue integration, but active tokens may persist in your tenant until explicitly revoked. Verify revocation is complete before proceeding.
2. Step 2: Detection. Query Salesforce event logs (EventLogFile object, RestApi and Login event types) for API calls originating from Klue's OAuth client ID during the suspected window of compromise. Look for bulk record queries against Account, Contact, Opportunity, and Lead objects executed outside normal business hours or at volumes inconsistent with typical Klue sync activity. Cross-reference source IPs in Salesforce login history against known Klue infrastructure. In connected platforms (Slack, Gong, etc.), review OAuth application access logs for anomalous query volume or off-hours activity attributed to Klue app tokens. Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) to structure the log review process.
3. Step 3: Eradication. Revoke all Klue OAuth tokens across every connected SaaS platform. Force-rotate any service account credentials or API keys that Klue had access to. Audit your own OAuth integration inventory (CIS 5.1: Establish and Maintain an Inventory of Accounts) for any other third-party integrations storing tokens in vendor-controlled environments, apply the same revocation review. Remove Klue Battlecards as an authorized connected app in all affected platforms. Verify no residual OAuth grants remain using each platform's connected app or third-party access audit tools.
4. Step 4: Recovery. After revocation, monitor Salesforce API logs for 72 hours for any continued anomalous access patterns that would indicate token reuse or additional compromised credentials. Validate that CRM data exports match expected record counts, flag any discrepancies as potential evidence of exfiltration scope. If Klue services are to be restored, require fresh OAuth authorization only after Klue provides a vendor security advisory confirming remediation. Apply NIST AU-9 (Protection of Audit Information), preserve all log exports as forensic artifacts before any log rotation occurs.
5. Step 5: Post-Incident. Conduct a third-party OAuth integration audit across your entire SaaS estate. For each integration, assess: whether the vendor stores your tokens in their environment, what data scopes are granted, and whether those scopes follow least privilege (NIST AC-6; CIS 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts). Establish a periodic OAuth grant review process (CIS 6.2: Establish an Access Revoking Process) targeting dormant or over-privileged third-party integrations. Require vendors handling OAuth tokens on your behalf to demonstrate credential lifecycle controls, including decommissioning of prototype and staging credentials (CWE-522 gap). Evaluate supply chain risk posture for all SaaS-to-SaaS integrations using D3-CRO (Credential Rotation) and D3-UAP (User Account Permissions) countermeasures.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to legal counsel, executive leadership, and your data protection officer immediately if Salesforce EventLogFile analysis confirms bulk export of Account, Contact, or Opportunity records containing PII (names, emails, phone numbers, company financials), as this likely triggers breach notification obligations under GDPR Article 33 (72-hour supervisory authority notification), CCPA, and applicable state breach notification laws — and if Icarus extortion contact has been received, escalate to law enforcement (FBI IC3) and outside counsel before responding to any extortion demand.
Recovery Notes	Do not re-authorize any Klue OAuth connection until Klue publishes a formal vendor security advisory specifically confirming that the compromised backend systems have been remediated, all harvested OAuth tokens have been invalidated server-side, and an independent third-party forensic review has been completed. During the 72-hour post-revocation monitoring window, treat any Salesforce RestApi EventLogFile entry with a CLIENT_ID matching Klue's previously registered OAuth application as evidence of active token reuse and re-enter containment immediately. Validate final CRM record counts against your last known-good backup to produce a defensible exfiltration scope estimate for breach notification and executive reporting purposes.
Forensic Artifacts	Salesforce EventLogFile object — RestApi event type CSV exports: contain CLIENT_ID, USER_ID, TIMESTAMP, ENTITY_NAME, and ROWS_PROCESSED fields that directly evidence which Salesforce objects (Account, Contact, Opportunity, Lead) Icarus queried via Klue's OAuth token and at what volume. | Salesforce Login History export (Setup > Login History): records source IP addresses, login timestamps, and OAuth application name for every Klue-initiated API session, enabling correlation of Klue OAuth activity against Icarus-controlled infrastructure IPs. | Salesforce Setup Audit Trail (Setup > Security > View Setup Audit Trail): captures the original OAuth authorization event for Klue Battlecards including the authorizing admin user, timestamp, and granted scopes — establishes when Icarus gained persistent access. | Gong and Chorus OAuth application access logs: if Klue's integration had scopes covering call recording platforms, these logs would show whether Icarus accessed recorded sales calls and deal intelligence beyond what Salesforce REST API logs capture — request via vendor admin portal before any vendor-side cleanup. | Google Workspace Admin audit log (admin.google.com > Reports > Audit > Token): records all OAuth token grants and access events for Google Drive connected via Klue, including the specific Drive file scopes accessed — critical for assessing whether sensitive documents in sales-related Drive folders were exfiltrated.

Per-Action IR Details

Step 1: Containment — Immediately audit all active OAuth grants in Salesforce (Setup > Connected Apps OAuth Usage) and revoke any token issued to Klue Battlecards. If your organization uses HubSpot, Gong, Slack, Zoom, Chorus, Clari, Google Drive, or SharePoint via Klue integrations, revoke those OAuth grants as well. Salesforce has already disabled the Klue integration, but active tokens may persist in your tenant until explicitly revoked. Verify revocation is complete before proceeding.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: Stop the bleeding by eliminating the attacker's access vector (Klue-issued OAuth tokens) before the threat actor can leverage any remaining valid tokens against Salesforce REST APIs or connected SaaS platforms.

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

Compensating: For teams without a SaaS management platform: run Salesforce SOQL via Developer Console — 'SELECT Id, AppName, UserId, LastUsedDate FROM ConnectedApplication' — to enumerate live OAuth grants. For Slack, use the Slack admin OAuth Apps page (api.slack.com/apps) filtered by 'Klue' to identify and revoke the app

token manually. For Google Drive, navigate to myaccount.google.com/permissions and remove Klue's access for each affected service account. Document each revocation with a timestamp screenshot as a chain-of-custody record.

Evidence: BEFORE revoking any token, export Salesforce EventLogFile records (RestApi and Login event types) for the full suspected compromise window using SOQL: 'SELECT Id, EventType, LogDate FROM EventLogFile WHERE EventType IN (\'RestApi\',\'Login\') AND LogDate >= LAST_N_DAYS:30'. Capture Salesforce Connected Apps OAuth Usage page as a screenshot showing Klue's client_id, token issuance timestamp, and last-used date. In Slack, export the OAuth app audit trail before removal. These records establish the token's lifespan and the data access window — they are overwritten or lost upon revocation and tenant cleanup.

Step 2: Detection — Query Salesforce event logs (EventLogFile object, RestApi and Login event types) for API calls originating from Klue's OAuth client ID during the suspected window of compromise. Look for bulk record queries against Account, Contact, Opportunity, and Lead objects executed outside normal business hours or at volumes inconsistent with typical Klue sync activity. Cross-reference source IPs in Salesforce login history against known Klue infrastructure. In connected platforms (Slack, Gong, etc.), review OAuth application access logs for anomalous query volume or off-hours activity attributed to Klue app tokens. Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) to structure the log review process.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Determine the scope of Icarus's access by reconstructing the full sequence of Salesforce REST API calls made under Klue's OAuth client ID, identifying which CRM objects were queried and at what volume.

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

Compensating: Without a SIEM, use the Salesforce Event Log File Browser (open-source, available at salesforce-elf.herokuapp.com or equivalent community tools) to download and parse EventLogFile CSVs locally. Filter RestApi logs on CLIENT_ID matching Klue's registered OAuth client ID. Use Python with the pandas library to pivot on TIMESTAMP, USER_ID, and ENTITY_NAME columns to identify bulk Account/Contact/Opportunity queries. For Gong and Chorus, request audit log exports from the vendor admin portal and grep for Klue's OAuth app name in the application_name or source_app fields. A two-person team can divide platform coverage: one analyst owns Salesforce logs, one covers connected SaaS platforms.

Evidence: Preserve raw EventLogFile CSV exports immediately — Salesforce retains event logs for only 30 days by default and they are not recoverable after rotation (NIST 800-61r3 §3.2 evidence preservation requirement). Capture the full Salesforce Login History (Setup > Login History) as a CSV, filtering on Klue's OAuth client ID, which records source IP, timestamp, and login type. In Gong and Chorus, download call recording access logs before any vendor-side cleanup. Cross-reference Klue's OAuth client_id against Salesforce's Named Credential and Remote Site Settings to determine what API endpoints were reachable under the granted scopes.

Step 3: Eradication — Revoke all Klue OAuth tokens across every connected SaaS platform. Force-rotate any service account credentials or API keys that Klue had access to. Audit your own OAuth integration inventory (CIS 5.1: Establish and Maintain an Inventory of Accounts) for any other third-party integrations storing tokens in vendor-controlled environments — apply the same revocation review. Remove Klue Battlecards as an authorized connected app in all affected platforms. Verify no residual OAuth grants remain using each platform's connected app or third-party access audit tools.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: Remove all artifacts of Icarus's access vector by eliminating every Klue OAuth token and associated credential from the environment, then verifying no residual grants persist across the full SaaS integration chain.

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Build a manual OAuth integration inventory using a spreadsheet: for each SaaS platform (Salesforce, HubSpot, Slack, Gong, Chorus, Clari, Google Drive, SharePoint, Zoom), document the connected app name, OAuth

client ID, granted scopes, and last-used date. Use each platform's native admin audit tool — Salesforce Connected Apps OAuth Usage, Google Workspace Admin > Security > API Controls, Slack Admin > Installed Apps — to enumerate and revoke. For service account API keys in Salesforce, navigate to Setup > Security > Named Credentials and Setup > Manage Connected Apps to identify any Klue-linked credentials beyond the standard OAuth flow. A two-person team can complete this sweep in 4-6 hours across all eight affected platforms.

Evidence: BEFORE rotating any service account credentials or API keys, export Salesforce Setup Audit Trail (Setup > Security > View Setup Audit Trail) which records all admin-level changes including OAuth app authorizations, Named Credential modifications, and Connected App installs — this log covers only the last 180 days and is not recoverable after the retention window. Screenshot each platform's connected app listing showing Klue's entry with its client_id and granted scopes BEFORE removal, as this documents the access scope Icarus could have leveraged. For SharePoint and Google Drive, export the OAuth app permission grants via Microsoft 365 Admin Center > Azure AD > Enterprise Applications and Google Admin > Security > API Controls respectively, before revocation alters the audit record.

Step 4: Recovery — After revocation, monitor Salesforce API logs for 72 hours for any continued anomalous access patterns that would indicate token reuse or additional compromised credentials. Validate that CRM data exports match expected record counts — flag any discrepancies as potential evidence of exfiltration scope. If Klue services are to be restored, require fresh OAuth authorization only after Klue provides a vendor security advisory confirming remediation. Apply NIST AU-9 (Protection of Audit Information) — preserve all log exports as forensic artifacts before any log rotation occurs.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: Restore normal operations only after verifying that all Klue OAuth tokens are invalidated and that no continued API access to Salesforce CRM objects is occurring under any credential set previously accessible to Icarus.

Controls: NIST AU-9 (Protection Of Audit Information), NIST AU-11 (Audit Record Retention), CIS 8.2 (Collect Audit Logs)

Compensating: Without automated monitoring, configure a Salesforce report on the EventLogFile object scoped to RestApi events, scheduled to run every 8 hours and emailed to the security team during the 72-hour watch period. Use the Salesforce Data Export tool (Setup > Data Export) to pull current record counts for Account, Contact, Opportunity, and Lead objects and compare against your last known-good backup count to quantify potential exfiltration scope. Archive all EventLogFile CSVs, Login History exports, and Setup Audit Trail exports to an off-platform location (encrypted S3 bucket or local encrypted drive) immediately — Salesforce's 30-day log retention makes these irreplaceable after the window closes.

Evidence: Before standing up any monitoring baseline, capture a final point-in-time snapshot of Salesforce EventLogFile (RestApi event type) covering the hour immediately following token revocation — this establishes the 'clean' baseline and would reveal any token reuse if Icarus had cached or cloned tokens outside Klue's backend. Preserve the Salesforce Login History export as a forensic artifact documenting the last successful Klue OAuth login, which anchors the end of the confirmed access window. Export and archive Gong and Chorus call access logs if those platforms were connected, as Icarus may have accessed recorded sales calls containing sensitive deal and contact intelligence beyond what Salesforce REST API logs alone would capture.

Step 5: Post-Incident — Conduct a third-party OAuth integration audit across your entire SaaS estate. For each integration, assess: whether the vendor stores your tokens in their environment, what data scopes are granted, and whether those scopes follow least privilege (NIST AC-6; CIS 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts). Establish a periodic OAuth grant review process (CIS 6.2: Establish an Access Revoking Process) targeting dormant or over-privileged third-party integrations. Require vendors handling OAuth tokens on your behalf to demonstrate credential lifecycle controls, including decommissioning of prototype and staging credentials (CWE-522 gap). Evaluate supply chain risk posture for all SaaS-to-SaaS integrations using D3-CRO (Credential Rotation) and D3-UAP (User Account Permissions) countermeasures.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Use the Icarus/Klue campaign as the forcing function for a structured lessons-learned review and systematic improvement of third-party OAuth governance across the SaaS estate, preventing recurrence via any similarly-positioned integration vendor.

Controls: NIST AC-6 (Least Privilege), NIST AC-20 (Use Of External Systems), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Build a SaaS OAuth register in a shared spreadsheet with columns: vendor name, OAuth client_id, platform connected, data scopes granted, token storage location (vendor-side vs. customer-side), last reviewed date, and least-privilege assessment (pass/fail). Prioritize any vendor — like Klue — that stores your OAuth tokens in their own backend infrastructure, as this mirrors the exact supply chain attack vector Icarus exploited. Use Google Workspace Admin SDK, Microsoft Graph API (Get-MgServicePrincipal), and Salesforce Connected Apps OAuth Usage to automate quarterly enumeration with a simple Python or PowerShell script rather than manual review. For vendor security questionnaires, add an explicit line item requiring disclosure of token storage architecture and staging credential decommissioning procedures.

Evidence: No volatile evidence capture applies to this post-incident planning phase. However, retain all forensic artifacts collected during Steps 1-4 — Salesforce EventLogFile exports, Login History CSVs, Setup Audit Trail, and connected app screenshots — for a minimum of 12 months to support regulatory breach notification obligations (e.g., GDPR 72-hour notification, CCPA, state-level PII breach laws) and any potential legal proceedings related to Icarus extortion activity. Document the lessons-learned output formally as an updated third-party integration risk acceptance record.

Detection Guidance

Primary detection surface is Salesforce EventLogFile (API type: RestApi, Login, ApexExecution). Query for: (1) OAuth client ID associated with Klue Battlecards making bulk queries against Account, Contact, Opportunity, or Lead objects, especially SELECT * or high-volume SOQL queries; (2) API calls from Klue's client ID at times inconsistent with your organization's Klue usage patterns; (3) Login events from Klue's connected app originating from IP ranges not previously associated with Klue infrastructure. In Gong, Slack, HubSpot, and other connected platforms, review OAuth application audit logs for Klue app activity with unusual data access volume. Behavioral indicators include: large record count responses to single API calls, repeated pagination through full CRM object exports, and API calls to data export or bulk query endpoints not used in normal Klue sync workflows. Apply D3-LAM (Local Account Monitoring) principles to OAuth-connected app accounts, treat third-party OAuth grants as accounts requiring the same anomaly monitoring as user accounts. D3-SFA (System File Analysis) principles apply to Salesforce debug logs and event log files, protect log integrity and ensure logs are retained per NIST AU-11 before any rotation event.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://www.bleepingcomputer.com/news/security/klue-oauth-breach-linked-to-icarus-salesforce-data-theft-attacks/`	BleepingComputer reporting on Icarus / Klue OAuth breach — source article, not a malicious URL	HIGH

Type	Value	Context	Confidence
URL	`https://reliaquest.com/blog/threat-spotlight-integration-abused-in-crm-data-theft`	ReliaQuest threat spotlight on Klue integration abuse — may contain additional IOCs and campaign TTPs	HIGH

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1195.002** — Compromise Software Supply Chain
- **T1530** — Data from Cloud Storage
- **T1567** — Exfiltration Over Web Service
- **T1657** — Financial Theft
- **T1539** — Steal Web Session Cookie
- **T1059.006** — Python
- **T1195** — Supply Chain Compromise
- **T1528** — Steal Application Access Token
- **T1078** — Valid Accounts

NIST-800-53R5

- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-7** — Least Functionality
- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes
- **SR-2** — Supply Chain Risk Management Plan
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **IA-8** — Identification and Authentication (Non-Organizational Users)

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A04:2021** — Insecure Design

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **5.2** — Use Unique Passwords
- **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(d)** — Person or Entity Authentication
- **164.308(a)(5)(ii)(D)** — Password Management

NIST-CSF-2

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

ISO-27001-2022

- **A.5.21** — Managing information security in the ICT supply chain
- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1195.002	Compromise Software Supply Chain	Initial-Access
T1530	Data from Cloud Storage	Collection
T1567	Exfiltration Over Web Service	Exfiltration
T1657	Financial Theft	Impact
T1539	Steal Web Session Cookie	Credential-Access
T1059.006	Python	Execution
T1195	Supply Chain Compromise	Initial-Access
T1528	Steal Application Access Token	Credential-Access
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
Security News	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
Klue Integrations | Slack, Hubspot, Gong & More	https://klue.com/product/integrations	T3
Klue OAuth breach linked to 'Icarus' Salesforce data theft attacks	https://www.bleepingcomputer.com/news/security/klue-oauth-breach-li...	T3
Klue Integration Abused in Salesforce Data Theft - ReliaQuest	https://reliaquest.com/blog/threat-spotlight-integration-abused-in-...	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 19:03 UTC by TJS Security Command Center