INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-19 13:51 UTC

Icarus Threat Actor Exploits Legacy Credentials and OAuth Tokens to Exfiltrate CRM Data from Klue-Connected Salesforce Environments

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0519
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Salesforce (REST API), Klue Battlecards integration infrastructure, connected enterprise CRM environments (confirmed victim: Huntress)
Published	2026-06-19T05:03:57
Discovery Source	Rss

Executive Summary

A threat actor tracked as Icarus breached Klue's integration infrastructure on June 11-12, 2026, by exploiting a dormant legacy service account credential to obtain OAuth tokens, then used those tokens to query Salesforce environments via the REST API and exfiltrate business contacts, pricing data, and sales messaging. At least one confirmed victim, cybersecurity firm Huntress, received an extortion demand with a 48-hour payment deadline. Organizations using Klue's Battlecards integration with Salesforce face direct exposure of competitively sensitive CRM data and potential extortion, with the root cause being systemic failures in non-human identity governance rather than a software vulnerability.

Technical Analysis

Icarus compromised Klue's third-party SaaS integration infrastructure by abusing a dormant legacy service account credential (CWE-287: Improper Authentication; CWE-522: Insufficiently Protected Credentials) that had not been decommissioned. The actor leveraged this credential to obtain OAuth access tokens with overly broad scopes (CWE-272: Least Privilege Violation; CWE-613: Insufficient Session Expiration), then used those tokens against the Salesforce REST API to bulk-retrieve CRM records including contacts, price quotes, and sales messaging. No CVE has been assigned; the attack vector is credential and token abuse, not a software vulnerability. MITRE ATT&CK techniques observed include T1078.004 (Valid Accounts: Cloud Accounts), T1528 (Steal Application Access Token), T1530 (Data from Cloud Storage), T1059.006 (Python-based automated query scripts), T1195.001 (Supply Chain Compromise), T1190 (Exploit Public-Facing Application),

T1550.001 (Use Alternate Authentication Material), T1567 (Exfiltration Over Web Service), and T1657 (Financial Theft/Extortion). No patch is applicable; remediation requires credential revocation, OAuth token invalidation, scope reduction, and enhanced third-party API monitoring. Attribution to Icarus carries medium confidence pending corroborating technical indicators. Sources are T3 (security trade press and vendor blog); no primary vendor advisory has been cited.

Action Checklist

1. Step 1: Containment. Immediately audit all active OAuth tokens granted to Klue's Battlecards integration and revoke every token associated with Klue within your Salesforce Connected Apps administration console. Disable the Klue connected app entirely until Klue provides an official remediation statement. Verify Salesforce's reported disabling of the Klue app applies to your org or take manual action if it does not.
2. Step 2: Detection. Query Salesforce event logs (EventLogFile, Setup Audit Trail, and API Usage logs) for bulk REST API reads originating from OAuth tokens associated with Klue or any unfamiliar connected app between June 11-12, 2026, and continuing forward. Look for anomalous data volumes on Contact, Opportunity, Quote, and related objects. Flag any API client not matching known, documented integration service accounts (NIST AU-6, CIS 8.2). Cross-reference against your NHI inventory for any service accounts with stale last-used dates that remain active.
3. Step 3: Eradication. Identify and permanently decommission every legacy service account credential across all SaaS integrations that is no longer actively managed or whose originating integration has been deprecated (NIST AC-2, CIS 5.3). Audit OAuth scopes for all remaining connected applications and reduce to least-privilege (NIST AC-6, CIS 3.3). Rotate all credentials associated with the Klue integration immediately. Implement token expiration policies so OAuth grants tied to inactive integrations expire automatically (aligned with NIST AC-12).
4. Step 4: Recovery. After revoking and rotating credentials, re-enable only explicitly approved, scope-limited integrations with documented business justification. Enable Salesforce Real-Time Event Monitoring if not already active and confirm alerting on abnormal API query volumes is operational (NIST SI-4, AU-2). Validate that no unauthorized exports occurred beyond the June 11-12 window by reviewing full EventLogFile exports for the 30 days prior. Document all affected records by type for potential regulatory notification assessment.
5. Step 5: Post-Incident. Conduct a full non-human identity (NHI) audit across all SaaS-to-SaaS integrations, cataloging every service account, OAuth grant, and API key with its owner, scope, last-used date, and expiration policy. Implement a recurring review cycle (at minimum quarterly) for third-party connected app permissions (NIST AC-2, AC-17, CIS 6.2). Establish monitoring baselines for third-party API access patterns and alert on deviation (NIST AU-6, AU-12). Evaluate vendor security attestations for all integration partners before reconnecting.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to legal counsel and initiate regulatory breach notification assessment immediately if the Salesforce Contact or Opportunity objects exposed by Icarus's bulk REST API queries are confirmed to contain PII governed by GDPR, CCPA, or sector-specific frameworks (HIPAA, PCI DSS), or if the extortion demand from Icarus is received, as both conditions trigger mandatory notification timelines and law enforcement reporting obligations that exceed IR team authority.
Recovery Notes	Before reconnecting any Klue or third-party Salesforce integration, require written confirmation from the vendor of the specific remediation steps taken to eliminate the compromised legacy service account credential and implement credential lifecycle controls, as Icarus's access vector was the vendor's infrastructure rather than your own. Monitor Salesforce RestApi and ConnectedApp EventLogFile entries daily for a minimum of 90 days post-recovery, alerting on any Connected App client ID not present in the approved NHI inventory or any single-session ROWS_PROCESSED count on Contact, Opportunity, or Quote objects exceeding your established baseline by more than 2 standard deviations. Given that Huntress — a cybersecurity firm with mature detection capabilities — was a confirmed victim, treat your own detection gap as a known weakness and assume the 90-day monitoring window may surface additional access events predating June 11 that were not initially visible in the 30-day EventLogFile export.
Forensic Artifacts	Salesforce EventLogFile — RestApi and ConnectedApp event types for June 1–12, 2026: primary record of Icarus's bulk SOQL queries against Contact, Opportunity, and Quote objects, including CLIENT_ID (Klue Connected App consumer key), ROWS_PROCESSED per request, URI patterns, and source IP addresses used to invoke the Salesforce REST API | Salesforce Setup Audit Trail for the 90-day period preceding June 11, 2026: captures any Connected App creation, OAuth scope modification, permission set assignment, or profile change associated with the dormant Klue service account credential prior to Icarus's exploitation, establishing the pre-compromise permission state | Salesforce Connected Apps OAuth Usage export (Setup > Connected Apps > OAuth Usage): point-in-time snapshot of all active OAuth tokens granted to Klue's Battlecards integration, including token issuance timestamps, associated Salesforce user, and granted scopes — volatile state destroyed upon token revocation | Salesforce Login EventLogFile entries for the Klue integration service account user: authentication timestamps, source IPs, and login types for the dormant credential Icarus exploited, enabling reconstruction of the initial access timeline and identification of any IP infrastructure associated with the Icarus campaign | Klue integration infrastructure logs and vendor-side audit trail (to be requested from Klue under incident response obligations): records of the June 11–12 breach of Klue's infrastructure, the specific legacy credential exploited, and the OAuth token issuance events that enabled Icarus to authenticate to victim Salesforce orgs — critical for establishing whether your org's tokens were issued before or during the confirmed breach window

Per-Action IR Details

Step 1: Containment — Immediately audit all active OAuth tokens granted to Klue's Battlecards integration and revoke every token associated with Klue within your Salesforce Connected Apps administration console. Disable the Klue connected app entirely until Klue provides an official remediation statement. Verify Salesforce's reported disabling of the Klue app applies to your org or take manual action if it does not.

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: Use Salesforce CLI (`sf org list auth`) or the Setup UI under Connected Apps > OAuth Usage to enumerate active tokens. Run a SOQL query via Developer Console: `SELECT Id, AppName, UserId, LastUsedDate FROM ConnectedApplication` and cross-reference against `SELECT Id, Name, LastModifiedDate FROM OAuthToken` (where available via Tooling API). For orgs without Real-Time Event Monitoring, pull EventLogFile records via REST: `GET /services/data/vXX.0/query?q=SELECT+LogFile+FROM+EventLogFile+WHERE+EventType='ConnectedApp'`. A 2-person team can complete token enumeration and revocation in the Connected Apps OAuth Usage panel within 30 minutes without any tooling budget.

Evidence: BEFORE revoking any token or disabling the Connected App, capture the full OAuth token state: export the Connected Apps OAuth Usage report from Setup > Connected Apps > OAuth Usage, recording AppName, User, LastUsedDate, and Scope for every active Klue token. Simultaneously export Salesforce EventLogFile entries for the ConnectedApp and API event types covering June 11–12, 2026, via REST API (`GET /services/data/vXX.0/sobjects/EventLogFile/`) — these log files rotate and will be destroyed on your org's retention schedule. Capture active session metadata from Setup > Session Management before any revocation action, as active session IDs linked to Icarus-controlled OAuth tokens will be unrecoverable post-termination.

Step 2: Detection — Query Salesforce event logs (EventLogFile, Setup Audit Trail, and API Usage logs) for bulk REST API reads originating from OAuth tokens associated with Klue or any unfamiliar connected app between June 11–12, 2026, and continuing forward. Look for anomalous data volumes on Contact, Opportunity, Quote, and related objects. Flag any API client not matching known, documented integration service accounts (NIST AU-6, CIS 8.2). Cross-reference against your NHI inventory for any service accounts with stale last-used dates that remain active.

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), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, query Salesforce EventLogFile directly via REST API and pipe to jq for filtering: `curl -H 'Authorization: Bearer ' 'https://.salesforce.com/services/data/v59.0/query?q=SELECT+LogFile,EventType,LogDate+FROM+EventLogFile+WHERE+EventType+IN+("API","RestApi","ConnectedApp")+AND+LogDate+=+2026-06-11T00:00:00Z' | jq`. Download the LogFile URLs and grep for `KLUE`, `Battlecards`, or high `ROWS_PROCESSED` values against Contact, Opportunity, or Quote objects. For Setup Audit Trail, export via Setup > View Setup Audit Trail and filter for `ConnectedApp`, `OAuthToken`, or `PermissionSet` changes on June 11–12. A Sigma rule targeting `EventType=RestApi AND RowsProcessed > 1000 AND ConnectedApp = Klue` applied against exported CSV logs covers the bulk-query detection pattern Icarus used.

Evidence: This is a detection/analysis step that does not alter live state, so no volatile pre-capture is required before running queries. However, note that Salesforce EventLogFile retention defaults to 30 days for most orgs (1 day for Developer Edition) — export ALL EventLogFile records for the June 1–12, 2026, window immediately before they age out. Key artifacts to extract: (1) RestApi event logs showing `CLIENT_ID` matching the Klue Connected App consumer key, `ROWS_PROCESSED` > baseline on Contact/Opportunity/Quote, and `URI` patterns consistent with bulk SOQL queries (e.g., `/services/data/vXX.0/query?q=SELECT+*+FROM+Contact`); (2) Setup Audit Trail entries for any OAuthToken creation, PermissionSet grant, or Connected App modification on or before June 11; (3) API Usage logs showing cumulative query volume per Connected App client ID to establish whether data exfiltration volume is consistent with the Klue integration's documented business purpose.

Step 3: Eradication — Identify and permanently decommission every legacy service account credential across all SaaS integrations that is no longer actively managed or whose originating integration has been deprecated (NIST AC-2, CIS 5.3). Audit OAuth scopes for all remaining connected applications and reduce to least-privilege (NIST AC-6, CIS 3.3). Rotate all credentials associated with the Klue integration immediately. Implement token expiration policies so OAuth grants tied to inactive integrations expire automatically (aligned with NIST AC-12).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), NIST AC-12 (Session Termination), CIS 5.3 (Disable Dormant Accounts), CIS 3.3 (Configure Data Access Control Lists)

Compensating: Export all Salesforce Connected App OAuth scopes via Tooling API: `SELECT Id, Name, OptionsAllowAdminApprovedUsersOnly, Scopes FROM ConnectedApplication`. For each app, compare declared scopes against documented integration requirements — any scope granting `full`, `api`, or `refresh_token` to a non-essential integration is a candidate for reduction. For legacy service accounts in Salesforce, run: `SELECT Id, Username, LastLoginDate, IsActive FROM User WHERE Profile.Name = 'Integration User' AND LastLoginDate < 2025-06-01` via Developer Console SOQL to surface dormant credentials matching the Icarus initial access vector. Credential rotation for the Klue-associated service account should include resetting the Salesforce-connected user password, regenerating the Connected App consumer secret, and invalidating all existing refresh tokens via the OAuth token revocation endpoint (`POST /services/oauth2/revoke`).

Evidence: BEFORE decommissioning any legacy service account or rotating credentials, capture: (1) the full authentication history for the Klue-associated Salesforce integration user via EventLogFile `Login` event type — filter on `USER_NAME` matching the service account and export all records dating back at least 90 days to establish whether the dormant credential Icarus exploited had any legitimate use prior to June 11; (2) the current OAuth token list including `refresh_token` issuance timestamps from the Tooling API or Setup > Connected Apps > OAuth Usage, preserving evidence of when the token Icarus weaponized was originally granted; (3) a snapshot of all Connected App scope configurations before modification, retained as forensic baseline for regulatory notification and post-incident review. These records establish the pre-compromise permission state and are required if breach notification obligations are triggered.

Step 4: Recovery — After revoking and rotating credentials, re-enable only explicitly approved, scope-limited integrations with documented business justification. Enable Salesforce Real-Time Event Monitoring if not already active and confirm alerting on abnormal API query volumes is operational (NIST SI-4, AU-2). Validate that no unauthorized exports occurred beyond the June 11–12 window by reviewing full EventLogFile exports for the 30 days prior. Document all affected records by type for potential regulatory notification assessment.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For orgs without Real-Time Event Monitoring licenses, implement compensating alerting by scheduling a daily cron job or Salesforce Flow that queries EventLogFile via REST API for the prior day's RestApi and ConnectedApp event logs, flags any `ROWS_PROCESSED` value exceeding a defined threshold (e.g., > 500 rows on Contact/Opportunity/Quote from any single Connected App client), and emails results to the security team. To validate the exfiltration window, download all EventLogFile records for May 12 through June 12, 2026 (the full 30-day prior period plus the confirmed compromise window), and use a Python script with pandas to sum `ROWS_PROCESSED` per `CLIENT_ID` per day — a spike on June 11–12 consistent with bulk Contact/Opportunity/Quote reads confirms Icarus's operational window. For regulatory scoping, cross-reference affected Salesforce object types (Contact, Opportunity, Quote) against your data classification inventory to determine whether PII, PHI, or contractual data was included in the exfiltrated records.

Evidence: Before re-enabling any integration or modifying the Salesforce environment, confirm that full EventLogFile exports covering May 12 through June 12, 2026, have been archived to immutable storage — these are the primary forensic record of Icarus's data access scope and will be required for any regulatory notification or legal hold. Additionally, capture a point-in-time export of all Salesforce object record counts (Contact, Opportunity, Quote, Account) from the Data Export Service or Data Loader to establish a post-incident baseline; any discrepancy from pre-incident counts may indicate record deletion or manipulation beyond the confirmed exfiltration. Preserve all Setup Audit Trail exports from this period, as they are only retained for 180 days in Salesforce and document the administrative actions Icarus may have taken to cover tracks (e.g., Connected App modifications, permission changes).

Step 5: Post-Incident — Conduct a full non-human identity (NHI) audit across all SaaS-to-SaaS integrations, cataloging every service account, OAuth grant, and API key with its owner, scope, last-used date, and expiration policy. Implement a recurring review cycle (at minimum quarterly) for third-party connected app

permissions (NIST AC-2, AC-17, CIS 6.2). Establish monitoring baselines for third-party API access patterns and alert on deviation (NIST AU-6, AU-12). Evaluate vendor security attestations for all integration partners before reconnecting.

NIST Phase: Post Incident

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

Controls: NIST AC-2 (Account Management), NIST AC-17 (Remote Access), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-12 (Audit Record Generation), CIS 6.2 (Establish an Access Revoking Process), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Build a NHI inventory using a spreadsheet seeded from Salesforce Tooling API queries: `SELECT Id, Name, LastModifiedDate FROM ConnectedApplication` and `SELECT Id, Username, LastLoginDate, IsActive FROM User WHERE UserType = 'Integration'`. For each entry, manually document owner, business justification, OAuth scopes, and last-used date. Schedule a quarterly calendar reminder for access review. For baseline establishment without a SIEM, export 30 days of RestApi EventLogFile data post-recovery, compute per-Connected-App daily average `ROWS_PROCESSED` using a Python/pandas script, and store the output as the deviation-alerting baseline. Apply the free Salesforce Shield Event Log File Browser (available via AppExchange at no charge for auditing purposes) to accelerate log review for a 2-person team without enterprise tooling.

Evidence: This post-incident step does not alter live system state, so no volatile pre-capture is required. However, the lessons-learned record itself constitutes a forensic artifact: document the precise timeline from Icarus's initial access via the dormant Klue service account credential (June 11, 2026) through detection, containment, and recovery, including every OAuth token revoked, every scope reduced, and every legacy credential decommissioned. This timeline, along with the full NHI inventory produced by this step, should be retained as evidence of remediation completeness for any regulatory inquiry or cyber insurance claim. Additionally, preserve Klue's official remediation statement and any vendor security attestations obtained before reconnecting integrations — these establish the due-diligence record required if a downstream incident recurs through the same vector.

Detection Guidance

Primary detection surface is Salesforce API and event logs. Query EventLogFile for API event type records between June 11-12, 2026, filtering for high-volume reads on Contact, Opportunity, Quote, and PricebookEntry objects from OAuth-authenticated sessions tied to the Klue connected app or any service account with 'integration' or 'klue' in the username. Look for sessions where a single OAuth client ID retrieved more than a few hundred records in a short window, particularly via SOQL SELECT * style queries. Review Setup Audit Trail for any connected app permission changes, new OAuth token grants, or scope modifications in the weeks preceding the incident. In your SIEM, correlate Salesforce API logs with outbound data transfer volumes; large payloads exiting to unfamiliar IP ranges during off-hours are a strong behavioral indicator. For behavioral threat hunting, apply MITRE ATT&CK T1528 (token theft) and T1530 (cloud data retrieval) hunt hypotheses: identify OAuth tokens issued to integration accounts that authenticated but whose parent service account had no recent human-login activity, consistent with a dormant credential being activated by an external actor. If you have Salesforce Shield or Real-Time Event Monitoring, alert on: API total calls per connected app exceeding a defined threshold per hour, first-time-seen OAuth client IDs performing data reads, and any bulk query against sensitive object types outside business hours. No public IOCs (IPs, domains, hashes) have been confirmed in source reporting at this time; treat absence of IOCs as a reason to rely on behavioral detection rather than signature-based blocking.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`No confirmed IOCs published in source reporting`	No IP addresses, domains, file hashes, or OAuth client IDs have been publicly attributed to the Icarus actor in available T3 sources. Detection should rely on behavioral indicators in Salesforce API logs rather than signature-based IOC matching.	LOW

Framework Mappings

MITRE-ATTACK

- **T1621** — Multi-Factor Authentication Request Generation
- **T1530** — Data from Cloud Storage
- **T1078.004** — Cloud Accounts
- **T1059.006** — Python
- **T1657** — Financial Theft
- **T1190** — Exploit Public-Facing Application
- **T1528** — Steal Application Access Token
- **T1195.001** — Compromise Software Dependencies and Development Tools
- **T1567** — Exfiltration Over Web Service
- **T1550.001** — Application Access Token

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
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **IA-5** — Authenticator Management
- **SR-2** — Supply Chain Risk Management Plan
- **SI-4** — System Monitoring

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
- **8.2** — Collect Audit Logs

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

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program
- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1621	Multi-Factor Authentication Request Generation	Credential-Access
T1530	Data from Cloud Storage	Collection
T1078.004	Cloud Accounts	Defense-Evasion
T1059.006	Python	Execution
T1657	Financial Theft	Impact
T1190	Exploit Public-Facing Application	Initial-Access
T1528	Steal Application Access Token	Credential-Access
T1195.001	Compromise Software Dependencies and Development Tools	Initial-Access
T1567	Exfiltration Over Web Service	Exfiltration
T1550.001	Application Access Token	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/salesforce-disables-klue-app.html	T3
	https://thehackernews.com/2026/06/salesforce-disables-klue-app.html	T3
Salesforce Data Thefts Continue via Klue App Compromise	https://www.darkreading.com/cyberattacks-data-breaches/salesforce-d...	T3
Attackers Steal Salesforce Data From Klue Battlecards Users	https://www.bankinfosecurity.com/attackers-steal-salesforce-data-fr...	T3
Klue Integration Abused in Salesforce Data Theft - ReliaQuest	https://reliaquest.com/blog/threat-spotlight-integration-abused-in-...	T3

Generated 2026-06-19 13:51 UTC by TJS Security Command Center