EOTISEC
ANALYTICAL INTELLIGENCE REPORT
EOTISEC Analytical Division

Report Title	**Klue / Icarus: OAuth-Based Supply Chain Compromise of Competitive Intelligence Platform Exposes CRM Data Across the Cybersecurity Industry**
Report Number	**EOTISEC-2026-046**
Supersedes	**N/A (initial report)**
Date of Report	**23 June 2026**
Coverage Period	**11 June 2026 to 23 June 2026**
Classification	**SENSITIVE BUSINESS DOCUMENT**
Originator	**EOTISEC Analytical Division**
Subject	**A newly emerged criminal extortion group designating itself Icarus, tentatively equated with the cluster Mandiant tracks as UNC6395, exploited a dormant legacy credential in the integration infrastructure of Klue, a Vancouver-based competitive intelligence SaaS platform, to harvest OAuth tokens for downstream customer environments. The group used those tokens to bulk-exfiltrate CRM data from Salesforce instances at a minimum of ten named organizations. Of those that have publicly disclosed, most are cybersecurity firms, though the composition of the broader victim pool remains unknown. Klue states the broader victim pool numbers in the hundreds. The stolen data is CRM business intelligence, not security product telemetry or credentials, but it is sufficient material for targeted phishing and social engineering against the affected organizations and their clients. The incident is contained as of 23 June 2026, though the June 22 publication deadline Icarus set has passed and whether they followed through is unconfirmed at time of drafting.**
Customer Sector	**Information Technology and Communications. Secondary: Financial Services, Defense Industrial Base via cybersecurity vendor exposure.**
Distribution	**Subscribers**

SECTION 1: SCOPE AND PURPOSE

This is the initial EOTISEC report on the Klue supply chain compromise, designated EOTISEC-2026-046. It covers the period from the first anomalous activity on June 11, 2026 through the report date of June 23, 2026. This is an early-stage product written deliberately close to a fast-moving incident. Readers should treat it as a point-in-time snapshot with several unresolved questions rather than a settled assessment.

The report draws on disclosures from Klue CEO Jason Smith (June 19, 2026), Huntress (June 17 and ongoing), ReliaQuest (June 21), BleepingComputer, CSO Online, Dark Reading, The Hacker News, SecurityWeek, TechCrunch, Infosecurity Magazine, The Register, and secondary advisory sources including Rescana and Ampcus Cyber. It also draws on the attribution history of UNC6395 from Mandiant and Mitiga reporting, and the broader Salesforce OAuth-abuse campaign history documented by those firms and Huntress. The report draws exclusively from open-source reporting, vendor disclosures, and market data. No classified sources were consulted.

The assessment is written for subscribers who operate cybersecurity programs, carry third-party SaaS vendor exposure, maintain Salesforce environments with third-party integrations, or track criminal extortion actors in the

cybersecurity space. The core analytic problem at this stage is that Klue has not disclosed how many of its customers were affected beyond the word hundreds, and several named victims have not yet published their own characterizations of what was taken. The report identifies what is known, what is inferred, what is claimed but unverified, and what remains genuinely open.

SECTION 2: KEY JUDGMENTS

Judgment 1: Confirmed Breach of Klue Integration Infrastructure — HIGH CONFIDENCE

We assess with **high confidence** that a threat actor gained unauthorized access to Klue's integration infrastructure on or about June 11, 2026, used a compromised legacy credential to obtain customer OAuth tokens, and used those tokens to query and exfiltrate data from connected Salesforce environments. This is confirmed by Klue's own CEO statement, independent analysis by Huntress and ReliaQuest including direct inspection of Salesforce API logs, and Salesforce's own detection of anomalous activity leading to platform-wide integration suspension on June 17.[1][2][3]

Judgment 2: Scale — HUNDREDS OF KLUE CUSTOMERS AFFECTED, EXACT COUNT UNKNOWN — LOW CONFIDENCE

We assess with **low confidence** on the precise count. Klue has not disclosed a number. Huntress, a confirmed victim, described the broader impact pool as hundreds of Klue customers. At least ten organizations have publicly confirmed their Salesforce data was accessed: Huntress, Recorded Future, Tanium, Jamf, HackerOne, Kudelski Security, Snyk, OneTrust, Sprout Social, and Insurity. Gong separately confirmed its own integration was abused to access internal licensed user data. At least one additional vendor has been identified in customer notifications but has not published a public statement as of the report date, possibly reflecting non-disclosure obligations. What is confirmed publicly represents only a subset of those notified.[4][5][6][7]

Judgment 3: Data Taken — BUSINESS CRM RECORDS, NOT SECURITY TELEMETRY — HIGH CONFIDENCE

We assess with **high confidence** that the data taken is business intelligence rather than security-sensitive material. Every affected organization that has published a disclosure characterizes the exposure as contact names, email addresses, job titles, phone numbers, business addresses, sales opportunity records, pricing quotes, and sales communications pulled from Salesforce. No confirmed victim has reported compromise of passwords, payment card data, security product telemetry, vulnerability data, or internal engineering material. This limit on immediate harm does not reduce the follow-on phishing and social engineering risk.[1][4][5][6]

Judgment 4: Attribution to Icarus — HIGH CONFIDENCE WITH CAVEATS ON LINEAGE

We assess with **high confidence** that the group calling itself Icarus conducted this attack. Attribution rests on a specific technical link: the Session Messenger ID in extortion emails sent to Huntress matched the ID posted on the Icarus dark-web leak site, and when Icarus updated that ID on their site, the corresponding update appeared in follow-up extortion emails, a correlation Huntress documented. The group publicly claimed the attack on June 19 on their Tor-based leak site. The caveat is on lineage. Rescana's advisory explicitly equates Icarus with UNC6395, the cluster Mandiant linked to the Salesloft Drift OAuth campaign of August 2025 that compromised approximately 760 Salesforce organizations. ReliaQuest, in its original analysis of the Klue incident, noted the technique closely mirrors UNC6395's Drift playbook but stopped short of confirming the link, citing insufficient evidence. The tooling in the Klue incident used a generic Python-urllib user agent and ordinary data-center IP infrastructure rather than the Tor routing and distinct user agents previously documented in UNC6395 activity. The relationship between Icarus and UNC6395 is treated as plausible but unconfirmed.[2][3][8][9][10]

Judgment 5: Initial Access Vector — CONFIRMED LEGACY CREDENTIAL — HIGH CONFIDENCE

We assess with **high confidence** that initial access came through a dormant, forgotten credential originally created by Klue for a prototype integration that was never deployed and never decommissioned. This is described in Klue's CEO statement and corroborated by Huntress's investigation. Once inside, the attacker pushed a code update to Klue's integration infrastructure that harvested OAuth tokens customers had authorized for the Klue Battlecards application. The attacker never needed to phish a Klue employee, exploit a vulnerability, or bypass MFA. They walked through an unlocked door nobody remembered existed.[1][2]

Judgment 6: Unauthorized Code — CONFIRMED BUT UNEXPLAINED — MODERATE CONFIDENCE

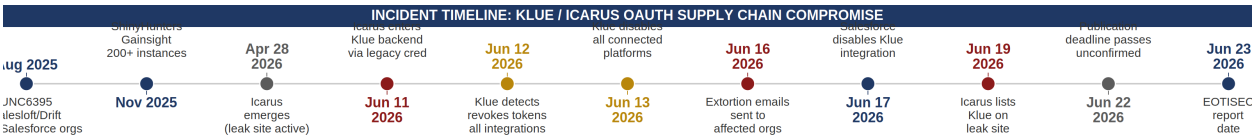
We assess with **moderate confidence** that the attacker modified Klue's code rather than only using existing access. Klue's CEO statement references removing unauthorized code as a remediation step, and Huntress's reconstruction describes the attacker pushing a code update capable of collecting OAuth tokens. Klue has not explained what the code did beyond token harvesting, how it was introduced, or whether it constituted a backdoor versus a one-time collection mechanism. This gap matters for assessing whether the attacker retained any access after Klue's containment actions. CrowdStrike has been engaged for forensics, and a conclusion is expected, but had not been published as of the report date.[1][2]

SECTION 3: SITUATION AND BACKGROUND

Klue is a Vancouver, British Columbia, Canada-based competitive intelligence platform with more than 250,000 users worldwide. Its core product, Klue Battlecards, aggregates competitive data and syncs it into customer sales and CRM environments, most commonly Salesforce. The integration works through OAuth 2.0 authorization, which means Klue holds tokens that grant it access to customer Salesforce environments as if it were the customer. That design is appropriate for the product's purpose. The security consequence is that Klue's integration infrastructure becomes a single point of failure for every customer's connected CRM.

The breach pattern here is not new. Klue is the third named integration application compromised to steal Salesforce data in roughly ten months. In August 2025, UNC6395 compromised Salesloft's GitHub environment, found OAuth tokens for the Drift email application using TruffleHog, and used those tokens to query Salesforce environments across approximately 760 customer organizations. In November 2025, ShinyHunters compromised Gainsight authentication tokens in a parallel operation affecting more than 200 Salesforce instances. The Klue case uses the same structural attack surface: a SaaS vendor with OAuth access to customer CRM environments, and a credential that persisted past its useful life.

The broader campaign context is relevant to subscriber exposure. The attacker in the Salesloft Drift case specifically targeted support case data in Salesforce, because organizations routinely paste plaintext credentials into support cases. AWS keys, Snowflake tokens, VPN credentials, and passwords stored in support ticket text were among the data taken. The Klue case does not appear to have targeted support cases specifically, and no victim has reported credential theft beyond the CRM contact data. That may reflect the scope of the OAuth permissions Klue's integration held, which was calibrated for competitive intelligence functions rather than full CRM access. The full scope of what Icarus queried inside each victim's Salesforce environment is not characterized in any public source.



LINCHPIN ASSUMPTION

This assessment assumes the Klue CEO statement and the Huntress forensic reconstruction accurately characterize both the initial access mechanism and the scope of the exfiltration. If the legacy credential story is incomplete and the attacker had a more persistent or deeper foothold in Klue's infrastructure, the exposure could

extend beyond what the current disclosures describe. The removal of unauthorized code is the single fact that most warrants this caveat. Klue has offered no detail on what that code did, whether it created backdoor access, or whether CrowdStrike's investigation has confirmed the environment is clean. Treating the environment as fully contained would be premature until that confirmation is published.

SECTION 4: ANALYSIS

4.1 The Attack Chain in Detail

The attack followed a sequence that ReliaQuest and Huntress reconstructed from Salesforce API logs and Klue's own notifications. On June 11, anomalous behavior appeared in Klue's integration infrastructure. The attacker used the legacy credential to access Klue's backend systems and pushed a code update designed to harvest OAuth tokens from the Klue Battlecards integration. Using those harvested tokens, the attacker authenticated to victim Salesforce environments as if they were the Klue integration service account.[1][2][3]

Inside each victim's Salesforce environment, the attacker ran automated Python scripts identifiable by a Python-urllib user agent string. The scripts first queried the Salesforce object catalog via GET /services/data/v59.0/sobjects to enumerate available data, then ran repeated queries against the REST API endpoint /services/data/v59.0/query, paginating through results using the QueryMore cursor. ReliaQuest observed a concentrated burst of nearly a thousand queries in a 15-minute window against at least one environment, with sustained exfiltration windows lasting more than six hours across the campaign.[3]

Klue detected the unauthorized activity on June 12 and began containment. By June 13 they had revoked OAuth credentials for all customers and disabled integrations with Salesforce, HubSpot, SharePoint, Zoom, Gong, Chorus, Clari, Google Drive, and Slack. Salesforce independently detected the anomalous activity and disabled the Klue Battlecards integration platform-wide on June 17. The first extortion emails reached affected organizations on June 16, sent from compromised mail servers belonging to Global Retail Brands, an Australian appliance retailer, under the alias mr bean. Icarus publicly listed Klue on its dark web leak site on June 19 and set a June 22 deadline for negotiations.[1][2][4][7]

4.2 What the OAuth Mechanism Means Practically

OAuth tokens are the operational core of this attack and deserve plain explanation. When an organization connects Klue to Salesforce, Salesforce issues a token that acts as a persistent authorization key. From Salesforce's perspective, any request bearing that token comes from Klue. There is no further authentication check. The token does not expire quickly by default, and it carries whatever permissions were granted to the Klue integration at setup time. Many enterprise integrations are granted broad scopes because administrators choose convenience over least privilege.

The consequence is that once Icarus held the harvested tokens, they had working, authenticated access to customer Salesforce environments with no phishing, no malware on customer endpoints, and no MFA challenge. Traditional authentication monitoring does not detect this because the login succeeded. The only signal is volumetric: the query rate was higher than a legitimate integration would produce, and the queries targeted objects that Klue would not normally touch at that scale. That signal was visible in Salesforce API logs, but only if those logs were being watched and only if someone knew what a legitimate Klue query pattern looked like. The attack ran for roughly 24 hours before containment, at a pace that made bulk extraction feasible.[2][3]

4.3 The Icarus Actor: What We Know and What We Do Not

Icarus appeared on the criminal extortion scene on April 28, 2026, by its own leak site's account. Before the Klue campaign, the site listed two victims: one from early May whose data was briefly hosted on gofile.io before expiring, and a second pending entry posted June 16 referencing Salesforce data. The operational security the group displayed was uneven. Huntress noted that the initial extortion email was signed mr bean before the actor sent a

follow-up correcting themselves with wrong session lol, suggesting either multiple operators sharing infrastructure or general operational sloppiness. The extortion emails were routed through compromised mail servers at three subsidiaries of Global Retail Brands in Australia, which the group did not appear to own or control in a sophisticated way.[2][4]

The Icarus-as-UNC6395 question is the most consequential attribution gap. UNC6395 is a cluster Mandiant tracked in connection with the August 2025 Salesloft Drift campaign. That campaign used Tor for routing and python-requests and Salesforce-CLI user agents, which are distinct from the Python-urllib and ordinary data-center hosting seen in the Klue case. If Icarus is UNC6395, the tooling shift might reflect deliberate retooling after the Drift campaign attracted public analysis. If Icarus is a different, newer group that adopted the same technique after Drift was publicly documented, that implies the OAuth-abuse playbook has diffused beyond UNC6395 and is now in wider circulation among financially motivated actors.[3][8][9]

On June 21, 2026, an unverified post on the ShinyHunters Telegram channel claimed responsibility for the Klue breach, which would connect Icarus to the broader ShinyHunters ecosystem. Huntress did not corroborate this claim, noting the Klue technique differed meaningfully from ShinyHunters' documented playbook of voice phishing employees into authorizing malicious connected apps. The Klue attack started with a stolen legacy service credential on the vendor side, not social engineering against a customer's employee. The ShinyHunters claim is treated here as unverified and potentially a false flag or attribution opportunism.[2][3]

4.4 Scale Figures and Why They Are Uncertain

The gap between the confirmed public disclosures and the stated potential scale is large and analytically important. The table below records the principal figures as stated by each party, without reconciling them.

Source	Figure	Basis
Klue CEO Jason Smith	Undisclosed number	CEO blog post June 19, 2026. No count given.
Huntress	Hundreds of customers	Huntress characterization to The Register, June 22, 2026.
Public confirmations	10 named organizations	Individual company disclosures through June 22, 2026.
Known Unattributed Vendor(s)	Notified via Klue customer alert; no public disclosure filed	One or more vendors received customer notifications and have not filed public disclosures. May reflect non-disclosure obligations or ongoing investigation. Count and scope unknown.
Gong	Internal licensed user data accessed	Names, titles, emails confirmed. No call recordings or transcripts affected.

The ten named organizations are a floor. The true count is likely higher, given Huntress described hundreds of customers as affected, though Huntress is itself a victim with a perspective on the incident rather than a neutral auditor. The hundred-plus characterization from Huntress is plausible given that Klue serves hundreds of enterprise customers and the attacker ran automated bulk queries rather than a targeted operation. The precise count will also depend on what qualifies as affected: some organizations may have had their tokens harvested but their Salesforce environments only lightly queried, or may not have stored meaningful data in the fields the attacker targeted.

4.5 The Security Vendor Concentration

Among organizations that have publicly disclosed impact, the victim list is weighted toward the cybersecurity sector. This may reflect Klue's customer base, selective disclosure behavior, or both, and it should not be read as describing the composition of the full victim population. Huntress, Recorded Future, Jamf, HackerOne, Kudelski Security, Snyk,

and Tanium are all security or security-adjacent companies. At least one additional unattributed vendor received customer notifications but has filed no public disclosure. Insurity is insurance software. Sprout Social is social media analytics. One plausible explanation for the security sector weighting is that competitive intelligence tools like Klue are heavily used in enterprise security sales, where cycles depend on capability comparisons and battlecard content. But because Klue has not disclosed its full customer list, this remains an inference rather than a confirmed reason.

The downstream risk worth noting is that CRM data from security vendors includes contact information, account relationships, and sales communications. That kind of data can support follow-on phishing or impersonation attempts directed at the affected vendors' customers. The extent to which any actor will exploit it is unknown at this stage.

4.6 The Unauthorized Code Question

This is the largest unresolved technical question in the current open-source picture. Klue's CEO described removing unauthorized code as part of the response without explaining what it was or what it did. Huntress's reconstruction characterized it as code capable of collecting OAuth tokens. But code that can be pushed to a backend system and collect tokens is also code that could create persistence, exfiltrate internal Klue data, or establish a callback channel.

No public source confirms that the unauthorized code did anything beyond what has been described. Until Klue or CrowdStrike publish a definitive characterization of what the code did and confirm that the environment is clean, this remains open. The fact that Klue immediately disabled all integrations and revoked all tokens limits the potential harm from any persistent capability, but does not eliminate it. Organizations that were Klue customers should be alert to any anomalous communication from Klue or its integration endpoints until the forensic conclusion is published.

4.7 Pattern of Comparable Activity

The Klue incident is the third entry in a documented series of SaaS integration compromises targeting Salesforce CRM data through third-party OAuth tokens over a ten-month period.

Campaign	Date	Actor	Mechanism and Scale
Salesloft / Drift	Aug 2025	UNC6395	Compromised Salesloft GitHub. TruffleHog found Drift OAuth tokens. Approximately 760 Salesforce organizations exfiltrated. Targeted support case credentials including AWS keys and passwords.
Gainsight	Nov 2025	ShinyHunters	Gainsight authentication tokens stolen. More than 200 Salesforce instances accessed.
Klue / Battlecards	Jun 2026	Icarus (possibly UNC6395)	Legacy credential used to harvest OAuth tokens. 10 or more named victims publicly confirmed. Hundreds more possible per Huntress. Data characterized as CRM business records by victims in their own disclosures; independent verification pending.

The pattern across all three is the same: a trusted third-party SaaS vendor with OAuth access to customer CRM environments, a credential or token that persisted beyond its intended lifecycle, and automated bulk exfiltration of CRM data. The Klue case differs from Drift in two structural ways. First, initial access came from inside Klue's infrastructure through Klue's own forgotten credential rather than through a compromise of a source code repository. Second, the data taken appears limited to standard CRM business fields rather than the support case credentials that made the Drift campaign especially damaging. Whether that reflects a different attacker or a different OAuth scope granted to Klue is unclear.

4.8 MITRE ATT&CK Mapping

The observed and reported behaviors map to the following ATT&CK techniques.

Technique	Name	Tactic	Basis
T1190	Exploit Public-Facing Application (integration endpoint)	Initial Access	Confirmed
T1078	Valid Accounts (harvested OAuth tokens)	Initial Access	Confirmed
T1528	Steal Application Access Token	Credential Access	Confirmed
T1059.006	Command and Scripting: Python	Execution	Confirmed via Python-urllib user agent
T1530	Data from Cloud Storage (Salesforce REST API)	Collection	Confirmed
T1567	Exfiltration Over Web Service	Exfiltration	Confirmed
T1136	Create Account (possible persistence)	Persistence	Assessed, not confirmed

SECTION 5: DECISION SUPPORT AND RECOMMENDATIONS

The following actions apply to any organization that used the Klue Battlecards integration with Salesforce. Klue revoked all OAuth tokens as part of its containment response, so the immediate active-access risk is addressed. The remaining actions address residual exposure and defensive posture going forward.

Immediate Verification

- Verify that the Klue OAuth integration has been fully revoked in your Salesforce environment. In Salesforce, navigate to Setup, then Manage Connected Apps, then OAuth Connected Apps. Locate the Klue Battlecards integration and confirm all tokens are revoked. Check for any unrecognized connected apps that may have been created by the attacker during the exfiltration window.
- Audit Salesforce API logs for the period June 11 through June 13, 2026 for anomalous query volume against any endpoint. Look specifically for Python-urllib user agent strings, bulk GET queries against /services/data/v59.0/query, and access from IP addresses in the Netherlands, France, or Ukraine. Klue's notification includes a non-exhaustive list of known attacker IP addresses.
- Treat unsolicited communications claiming to be from Klue, from any of the affected security vendors, or referencing the incident with urgency as potentially social engineered. Icarus has signaled it will contact affected organizations directly. The June 22 publication deadline has passed. Whether data was released is not confirmed at report time, but the actor holds the material.

SaaS Integration Hygiene

- Audit every third-party application with OAuth access to your Salesforce or other CRM environments. Revoke any integration that is no longer in active use. Legacy credentials and forgotten OAuth grants are the root cause in this case and in the Drift campaign before it. This audit should be a calendar item, not a one-time project.
- Enforce least-privilege OAuth scopes for all integration applications. An integration that needs to read competitive data does not need api-level access or refresh token generation. Scopes granted at setup

frequently exceed what the integration actually requires because requesting maximum access is the path of least resistance for the integrating vendor.

- Enable and monitor Salesforce API activity logs. The Klue exfiltration was visible in log data to organizations that had logging enabled and were watching it. A burst of nearly a thousand queries in 15 minutes from a known integration account is a detectable anomaly. If API logs are not being ingested into a SIEM or reviewed on a cadence, that is the highest-priority infrastructure gap this incident reveals.
- Restrict integration service accounts to known IP allowlists where the integrating vendor's infrastructure is predictable. A legitimate Klue integration does not need to authenticate from Ukrainian data centers.

Decision Support

The most time-sensitive decision for any organization that used Klue is verifying that the stolen data has been scoped. Every organization that published a disclosure characterized the exposure as limited to CRM business fields and stated that products, infrastructure, and sensitive security data were not affected. That characterization is self-reported and was made during or shortly after the incident. Subscribers should seek written confirmation from Klue and from CrowdStrike's forensic review before closing their own incident tracking on this event. The unauthorized code question is the specific item that warrants a written answer before an organization can treat this as resolved.

Organizations not using Klue should treat this incident as a prompt to conduct the SaaS OAuth integration audit described above. The Drift, Gainsight, and Klue cases suggest a pattern is forming. Three incidents do not make a law, but the structural conditions that enabled all three, specifically SaaS vendors holding OAuth access to CRM environments with no credential lifecycle discipline, remain broadly present. Future incidents following a similar template are plausible given that the technique has now been publicly documented and repeated. A subscriber that has not audited its third-party OAuth grants is carrying an exposure that is now well-characterized and demonstrably exploitable.

SECTION 6: INFORMATION GAPS AND COLLECTION REQUIREMENTS

This report is an early-stage product on a recent event. The following gaps are the primary sources of analytic uncertainty and will drive the update cycle.

- Total victim count. Klue has not disclosed how many of its customers were affected. A complete count with sector and geographic breakdown would allow a fuller assessment of downstream phishing risk. Collection priority: HIGH.
- Forensic conclusion on the unauthorized code. Klue's reference to removing unauthorized code is the single most important open technical question. Whether it was limited to a token harvester or included a backdoor or persistence mechanism will determine whether the containment story holds. CrowdStrike has been engaged but had not published findings as of report date. Collection priority: HIGH.
- Icarus lineage. The connection between Icarus and UNC6395 is suggested by Rescana but uncorroborated by ReliaQuest and Huntress. Confirming or excluding UNC6395 involvement would affect how to assess future risk from this actor and whether it is the same group responsible for the Drift and Gainsight campaigns. Collection priority: MODERATE.
- Whether Icarus leaked the data after the June 22 deadline. At report time this is unknown. If they published, the phishing risk and reputational harm escalate. If they did not, it may indicate negotiations are in progress or the group backed down. Collection priority: MODERATE.
- Unattributed vendor scope. One or more vendors received customer notifications but have not published disclosures, possibly due to non-disclosure obligations or active investigation. The scope of data accessible through their Klue integrations is unknown. Collection priority: MODERATE.
- The Gong integration scope. Gong separately disabled its Klue integration and reported that internal licensed user data was accessed. Gong stated no call recordings or transcripts were affected, but that

statement has not been confirmed by an independent forensic party. Call recordings and transcripts are substantially more sensitive than contact records. Collection priority: LOW.

SECTION 7: SOURCE SUMMARY STATEMENT

This assessment rests on a mix of primary vendor disclosures, forensic analysis by affected organizations, secondary security reporting, and extortion actor communications shared by Huntress. Source reliability is uneven and treated as such throughout. The Klue CEO statement, the Huntress forensic blog post, and the ReliaQuest threat spotlight are primary sources with direct access to the incident data and carry the most analytic weight. The Salesforce alert and the Gong statement are primary sources at high credibility. Secondary outlets including BleepingComputer, CSO Online, SecurityWeek, The Register, Dark Reading, and TechCrunch are treated as high-credibility aggregators whose reporting has been consistent and independently corroborated across accounts.

The Rescana advisory equating Icarus with UNC6395 is treated as a plausible characterization requiring further corroboration rather than a settled attribution, because its basis is not fully explained and conflicts with the tooling analysis from ReliaQuest. The ShinyHunters Telegram claim of responsibility is treated as unverified and potentially opportunistic. Scale figures for the potential victim pool originate from Huntress's characterization to The Register and are not independently audited. The ten confirmed named organizations are verified against their own published statements. One or more unattributed vendors are noted on the basis of third-party reporting of customer notifications only and have not been confirmed by the vendors themselves as of report date.

SECTION 8: ANALYTIC TRADECRAFT SELF-CERTIFICATION

Requirement	Status
Objectivity: free of advocacy, personal preference, or policy bias	CONFIRMED
Independence of political consideration: no judgment shaped to support a particular outcome	CONFIRMED
Timeliness: source material is current and the report is actionable	CONFIRMED. Source material current to June 23, 2026. Report is explicitly early-stage and flagged as such.
Based on all available sources: gaps documented in Section 6	CONFIRMED
Source credibility described: source quality addressed in Section 7	CONFIRMED
Uncertainty expressed: probability and confidence language conforms to ICD 203 standards	CONFIRMED. Confidence levels stated and differentiated across all six Key Judgments.
Assumptions distinguished from facts: linchpin assumption identified	CONFIRMED. One LINCHPIN ASSUMPTION identified in Section 3.
Alternatives incorporated: competing hypotheses addressed	CONFIRMED. Icarus vs. UNC6395 vs. ShinyHunters lineage addressed in Sections 2 and 4.3. Unauthorized code scope addressed in Section 4.6.
Customer relevance addressed: business impact stated by category	CONFIRMED. Security vendor concentration and downstream social engineering risk addressed in Section 4.5.
Decision support included: time-sensitive actions, ownership, and cost of inaction	CONFIRMED. Section 5 decision support paragraph with named decision owners.

Clear and logical argumentation: main message stated up front in Key Judgments	CONFIRMED
Source verification: primary-source or multi-link corroboration	CONFIRMED. ShinyHunters Telegram claim flagged as unverified. Rescana UNC6395 equation flagged as plausible but uncorroborated.

SECTION 9: ENDNOTES — VERIFIED SOURCE CHAIN

[1] Klue CEO Jason Smith. An Update on the Recent Klue Security Incident. June 19, 2026. Highest credibility. Primary vendor statement. CEO characterization of legacy credential, unauthorized code removal, and scope limitation. https://klue.com/blog/an-update-on-recent-klue-security-incident

[2] Huntress. Cybercrime Breaches Klue: Salesforce Data Impacted for Many Victims, including Huntress. June 17 and ongoing. Highest credibility for forensic reconstruction, Salesforce API log analysis, Icarus Session Messenger ID attribution, and the hundreds characterization. https://www.huntress.com/blog/klue-breach-investigation

[3] ReliaQuest. Klue Integration Abused in Salesforce Data Theft. June 21, 2026. High credibility. Primary technical reconstruction: Python-urllib user agent, query volume, 24-hour exfiltration window, 1,000-query burst, UNC6395 comparison, ShinyHunters alternative. https://reliaquest.com/blog/threat-spotlight-integration-abused-in-crm-data-theft

[4] BleepingComputer. Klue OAuth breach linked to Icarus Salesforce data theft attacks. June 18, 2026. High credibility. Source chain for Icarus extortion email content and alias mr bean. Global Retail Brands mail server detail. https://www.bleepingcomputer.com/news/security/klue-oauth-breach-linked-to-icarus-salesforce-data-theft-attacks/

[5] BleepingComputer. Klue OAuth breach victim list grows as Icarus hackers claim attack. June 19, 2026. High credibility. Victim list growth and Icarus public claim on leak site. https://www.bleepingcomputer.com/news/security/klue-oauth-breach-victim-list-grows-as-icarus-hackers-claim-attack/

[6] SecurityWeek. Cybersecurity Firms Impacted by Klue Supply Chain Attack. June 19, 2026. High credibility. Huntress and Recorded Future disclosures. https://www.securityweek.com/cybersecurity-firms-impacted-by-klue-supply-chain-attack/

[7] SecurityWeek. More Cybersecurity Firms Disclose Impact From Klue Hack. June 22, 2026. High credibility. HackerOne, Huntress, Jamf, OneTrust, Recorded Future, Snyk, Tanium confirmed. https://www.securityweek.com/more-cybersecurity-firms-disclose-impact-from-klue-hack/

[8] Rescana. Klue OAuth Integration Breach Exposes Salesforce Customer Data in Icarus Supply Chain Attack. June 21, 2026. Moderate credibility. Source for Icarus and UNC6395 equation and attack chain timeline. UNC6395 equation not independently confirmed by ReliaQuest or Huntress. https://www.rescana.com/post/klue-oauth-integration-breach-exposes-salesforce-customer-data-in-icarus-supply-chain-attack

[9] Mitiga. ShinyHunters and UNC6395: Inside the Salesforce and Salesloft Breaches. March 5, 2026. High credibility. UNC6395 Mandiant tracking history, Drift OAuth token mechanism, TruffleHog GitHub reconnaissance, Tor routing and user agent signatures for comparison to Klue tooling. https://www.mitiga.io/blog/shinyhunters-and-unc6395-inside-the-salesforce-and-salesloft-breaches

[10] Huntress Threat Library. ShinyHunters Threat Actor Profile. Accessed June 23, 2026. High credibility. Drift Salesloft 760 organization count, Gainsight 200-plus count, Anodot 2026 activity, UNC6395 cluster history. https://www.huntress.com/threat-library/threat-actors/shinyhunters

[11] Recorded Future. The Klue Security Incident and Its Impact on Recorded Future. June 17, 2026. Primary source, high credibility. Incident scope characterization and remediation steps. https://www.recordedfuture.com/blog/klue-security-incident

[12] HackerOne. Security Advisory: HackerOne Response to the Klue Breach. June 19, 2026. Primary source, high credibility. Data segmentation confirmation. No vulnerability data in CRM. https://www.hackerone.com/security-updates/klue-2026-06

[13] The Hacker News. Salesforce Disables Klue App Integration After OAuth Token Abuse Exposes Customer Data. June 22, 2026. High credibility. Salesforce alert text and Gong disclosure. https://thehackernews.com/2026/06/salesforce-disables-klue-app.html

[14] The Register. Security shops among the hundreds of Klue hack victims. June 22, 2026. High credibility. Kudelski Security addition to named victim list and Huntress hundreds characterization. https://www.theregister.com/cyber-crime/2026/06/22/security-shops-among-the-hundreds-of-klue-hack-victims/5259743

[15] TechCrunch. Klue hack results in data breach at several cybersecurity firms. June 22, 2026. High credibility. Gong, Jamf, HackerOne, Insurity, OneTrust, Recorded Future, Snyk, Sprout Social, Tanium confirmed. https://techcrunch.com/2026/06/22/klue-hack-results-in-data-breach-at-several-cybersecurity-firms/

[16] Dark Reading. Salesforce Data Thefts Continue via Klue App Compromise. June 22, 2026. High credibility. Global Retail Brands mail infrastructure detail. Klue as the third Salesforce integration abuse case. https://www.darkreading.com/cyberattacks-data-breaches/salesforce-data-thefts-klue-app-compromise

[17] Infosecurity Magazine. Klue Breach Enables Hackers to Compromise Cybersecurity Firms via OAuth Tokens. June 22, 2026. High credibility. ReliaQuest first-detector note. Salesforce June 17 platform disable. https://www.infosecurity-magazine.com/news/klue-breach-compromise/

[18] CSO Online. Klue breach exposed Salesforce CRM data through stolen OAuth tokens. June 22, 2026. High credibility. Salesforce statement, unauthorized code reference, Icarus attribution analysis. https://www.csoonline.com/article/4187907/klue-breach-exposed-salesforce-crm-data-through-stolen-oauth-tokens.html

[19] Rescana. Salesloft Drift OAuth Token Breach Enables Salesforce Data Theft in UNC6395 Icarus Attack Campaign. August 2026 advisory entry. Moderate credibility. Retrospective characterization equating UNC6395 with Icarus and connecting the August 2025 and June 2026 campaigns. Used here for the UNC6395 equation only. https://www.rescana.com/post/salesloft-drift-oauth-token-breach-enables-salesforce-data-theft-in-unc6395-icarus-attack-campaign-august-2026

[20] Hackread. Salesforce Disables Klue Integration After OAuth Token Theft Hits Customer Data. June 2026. High credibility for historical context: UNC6395 August 2025 Drift campaign and ShinyHunters November 2025 Gainsight campaign. https://hackread.com/salesforce-disables-klue-integration-oauth-token-data/

[21] MLQ News. Klue Supply-Chain Breach Exposes Salesforce Data at HackerOne, Huntress, and Seven Other Firms. June 22, 2026. High credibility. Synthesis and confirmation of nine named organizations. https://mlq.ai/news/klue-supply-chain-breach-exposes-salesforce-data-at-hackerone-huntress-and-seven-other-firms/

EOTISEC Analytical Division | EOTISEC-2026-046 | Klue / Icarus OAuth Supply Chain Compromise