INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-16 07:19 UTC

ShinyHunters Targets Council of Europe: 429K Documents, Active Extortion Deadline, and a Pattern of Institutional Escalation

DATA BREACH | **HIGH** | CVSS 9.5

SCC Item ID	SCC-DBR-2026-0175
Type	Data Breach
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Council of Europe internal HR and payroll systems; Oracle PeopleSoft (related ShinyHunters campaign context); Salesforce Aura; Salesloft Drift; Snowflake (prior campaigns)
Published	2026-06-15T12:37:11
Discovery Source	Rss

Executive Summary

ShinyHunters, a financially motivated threat group with a documented history of large-scale data extortion, has publicly claimed the exfiltration of over 429,000 documents from the Council of Europe, including HR, payroll, medical, and financial records spanning roughly 15 years for more than 10,000 staff members. The Council of Europe has confirmed it is investigating the claims but has not validated or denied them as of the discovery date. With a public extortion deadline of June 16, 2026, organizations sharing data relationships with the Council of Europe face immediate third-party exposure risk, and the breadth of sensitive personnel data raises serious regulatory and reputational consequences if the claim is substantiated.

Technical Analysis

ShinyHunters (also tracked as UNC6395 in the context of Salesforce and Salesloft campaigns) has claimed exfiltration of 429,000+ documents from Council of Europe internal HR and payroll systems. No CVE is directly associated with this incident. The breach characteristics map to CWE-284 (Improper Access Control), CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor), and CWE-269 (Improper Privilege Management). Relevant MITRE ATT&CK techniques include T1078 (Valid Accounts), T1213 (Data from Information Repositories), T1530 (Data from Cloud Storage), T1041 (Exfiltration Over C2 Channel), T1567.002 (Exfiltration to Code Repository), T1190 (Exploit Public-Facing Application), T1486 (Data Encrypted for Impact), and T1657 (Financial Theft). ShinyHunters' broader campaign context includes exploitation of Oracle PeopleSoft

deployments, Salesforce Aura misconfigurations, Salesloft Drift integrations, and Snowflake-hosted environments. The group's methodology follows a consistent pattern: gain initial access via valid accounts or public-facing application exploitation, exfiltrate sensitive data at scale, then apply public extortion pressure with a stated deadline before releasing data. The claimed data scope, medical, financial, and HR records over a 15-year window, suggests access to a deeply integrated HR/payroll platform, consistent with Oracle PeopleSoft or equivalent enterprise HR infrastructure. Attribution is based solely on ShinyHunters' own public claim; independent technical validation has not been publicly confirmed as of the discovery date.

Action Checklist

1. Step 1: Containment, If your organization has data-sharing, employment, or contractual relationships with the Council of Europe, treat that data as potentially compromised. Audit outbound data flows and shared credential stores tied to Council of Europe integrations immediately. If your environment runs Oracle PeopleSoft, Salesforce Aura, Salesloft Drift, or Snowflake, review those surfaces for indicators of unauthorized access consistent with ShinyHunters' TTPs (T1078, T1190). Isolate any shared service accounts that touch these platforms pending review.
2. Step 2: Detection, Query identity and access management logs for anomalous authentication events against HR, payroll, or document management systems: focus on off-hours access, bulk document retrieval (T1213), and large outbound data transfers (T1041, T1567.002). Review Snowflake, Salesforce, and PeopleSoft audit logs for access patterns matching T1530 (cloud storage data access). Correlate against AU-6 (Audit Record Review) requirements. Enable alerts on mass download or export events from document repositories. Check for lateral movement from external-facing application servers consistent with T1190.
3. Step 3: Eradication, Rotate all credentials for HR, payroll, and document management systems, prioritizing service accounts and administrative accounts (D3-CRO: Credential Rotation). Enforce MFA on all administrative and remote access paths to HR/payroll platforms (D3-MFA; CIS 6.3, 6.4, 6.5; NIST AC-17). Review and tighten access control lists on document repositories to enforce least privilege (NIST AC-6; CIS 3.3). Audit and revoke any dormant or over-privileged accounts (CIS 5.3, 5.4; NIST AC-2). Disable or restrict public-facing application endpoints not required for operations (consistent with T1190 mitigation).
4. Step 4: Recovery, Validate that access control changes are in effect across all HR and payroll system tiers. Confirm audit logging is active and centralized per NIST AU-2, AU-12, and CIS 8.2. Run a privileged account review against your account inventory (CIS 5.1) to confirm no residual unauthorized accounts remain. Monitor for secondary extortion contact, data publication attempts, or downstream credential abuse using identity threat detection tooling. Establish a watch on ShinyHunters' known leak sites for publication of claimed data as the June 16, 2026 deadline approaches.
5. Step 5: Post-Incident, Conduct a gap assessment against NIST AC-6 (Least Privilege), AC-3 (Access Enforcement), and AU-6 (Audit Record Review) to identify control failures that may have permitted bulk data access. Evaluate third-party data-sharing agreements and vendor access controls (NIST AC-20). Implement or validate D3-UAP (User Account Permissions) and D3-LAM (Local Account Monitoring) countermeasures. Review data retention scope; 15-year data exposure suggests retention policy enforcement gaps (CIS 3.4). Brief legal and communications teams on extortion response protocol before the deadline.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to legal, DPO, and senior leadership if any of the following are confirmed: Council of Europe data-sharing relationship exists with your organization, any ShinyHunters IOC matches activity in your HR/payroll or cloud data platform logs, or the June 16, 2026 extortion deadline passes without Council of Europe confirmation of containment — all scenarios involving HR, payroll, or medical PII for EU staff trigger GDPR Article 33 72-hour breach notification obligations.
Recovery Notes	After eradication, maintain elevated monitoring of Snowflake, PeopleSoft, and Salesforce authentication logs for a minimum of 90 days beyond the June 16, 2026 deadline, as ShinyHunters has a documented pattern of re-accessing environments after initial disclosure to maximize extortion leverage. Verify data integrity of HR and payroll records against known-good backups to detect any tampering that may have accompanied exfiltration. Coordinate with the Council of Europe's own incident response team (if a data-sharing relationship exists) to align on breach notification timelines and shared IOC disclosure under applicable data processing agreements.
Forensic Artifacts	Snowflake ACCOUNT_USAGE.ACCESS_HISTORY table: rows showing BYTES_WRITTEN_TO_RESULT spikes and QUERY_TEXT containing bulk SELECT or COPY INTO EXTERNAL STAGE commands against HR/payroll schema tables, timestamped against the suspected ShinyHunters access window | Oracle PeopleSoft PSACCESSLOG and PSAUDIT database tables: records of mass row-level access to EMPLID-keyed tables (employee HR, payroll, medical data) from non-standard operator IDs or off-hours timestamps consistent with bulk exfiltration | Salesforce Aura component server-side logs and Event Monitoring API logs: entries showing unauthenticated or anomalous Aura endpoint invocations (`/aura?r=` URIs) with large response payloads, consistent with ShinyHunters' known Salesforce Aura exploitation pattern | Perimeter NetFlow or firewall session logs: large-volume outbound TCP sessions (>100MB) to non-corporate destination IPs from HR/payroll application server network segments, time-correlated with the Snowflake or PeopleSoft access anomalies | Windows Security Event Log Event ID 4648 (Logon Using Explicit Credentials) and Event ID 4624 Type 3 (Network Logon) on document repository and HR application hosts: lateral movement indicators from external-facing web servers to internal data tiers consistent with post-exploitation pivoting after initial access via T1190

Per-Action IR Details

Step 1: Containment — If your organization has data-sharing, employment, or contractual relationships with the Council of Europe, treat that data as potentially compromised. Audit outbound data flows and shared credential stores tied to Council of Europe integrations immediately. If your environment runs Oracle PeopleSoft, Salesforce Aura, Salesloft Drift, or Snowflake, review those surfaces for indicators of unauthorized access consistent with ShinyHunters' TTPs (T1078, T1190). Isolate any shared service accounts that touch these platforms pending review.

NIST Phase: Containment

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

Controls: NIST AC-2 (Account Management), NIST AC-20 (Use Of External Systems), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Without a SIEM, run PowerShell on Windows: `Get-ADUser -Filter * -Properties LastLogonDate,ServicePrincipalNames | Where-Object {$_.ServicePrincipalNames -like '*PeopleSoft*' -or

$_.ServicePrincipalNames -like '*Salesforce*' -or $_.ServicePrincipalNames -like '*Snowflake*'}` to enumerate service accounts touching these platforms. For Snowflake, run `SELECT * FROM SNOWFLAKE.ACCOUNT_USAGE.LOGIN_HISTORY WHERE EVENT_TIMESTAMP > DATEADD(day, -30, CURRENT_TIMESTAMP()) ORDER BY EVENT_TIMESTAMP DESC;` directly in the Snowflake console. Use osquery on Linux hosts: `SELECT * FROM logged_in_users;` and review /var/log/auth.log for OAuth or API token activity tied to external integrations.

Evidence: Before isolating any shared service account, capture: (1) active sessions and token state for the account in PeopleSoft, Salesforce Aura, and Snowflake consoles — screenshot or export session tables; (2) current outbound network connections from integration hosts using `netstat -ano` (Windows) or `ss -tunap` (Linux) to document live data-flow endpoints; (3) Snowflake QUERY_HISTORY for the past 90 days filtered to the service account (`SELECT * FROM SNOWFLAKE.ACCOUNT_USAGE.QUERY_HISTORY WHERE USER_NAME = '';`); (4) Salesforce login history export for the connected app credential. These are volatile or time-limited log sources that will age out or be overwritten once the account is disabled.

Step 2: Detection — Query identity and access management logs for anomalous authentication events against HR, payroll, or document management systems: focus on off-hours access, bulk document retrieval (T1213), and large outbound data transfers (T1041, T1567.002). Review Snowflake, Salesforce, and PeopleSoft audit logs for access patterns matching T1530 (cloud storage data access). Correlate against AU-6 (Audit Record Review) requirements. Enable alerts on mass download or export events from document repositories. Check for lateral movement from external-facing application servers consistent with T1190.

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 SIEM correlation, use native platform audit logs directly: In Snowflake, query `SNOWFLAKE.ACCOUNT_USAGE.ACCESS_HISTORY` filtering for `BYTES_WRITTEN_TO_RESULT > 10000000` to surface bulk export events. In Salesforce, pull Setup Audit Trail and Login History CSVs and filter in Excel or Python (`pandas`) for off-hours login timestamps and bulk Report exports. For PeopleSoft, query the PSACCESSLOG and PSOPRDEFN audit tables. For document management exfil, deploy Sysmon with Event ID 11 (FileCreate) and Event ID 23 (FileDelete) monitoring on document repository servers, and alert on high-volume file access within short time windows using a Sigma rule targeting mass file open events.

Evidence: No live-state alteration in this step — detection is passive. However, document and preserve the following before any downstream containment actions overwrite them: (1) Snowflake ACCESS_HISTORY rows showing rows_produced and bytes_written_to_result for the suspect time window — export to CSV immediately as this table retains only 365 days and can be pruned; (2) Salesforce Event Monitoring logs (if licensed) or Setup Audit Trail exports covering the 90 days prior to discovery — Salesforce purges these on rolling windows; (3) Oracle PeopleSoft IB_MONITOR and PSACCESSLOG database tables covering the 15-day window before discovery; (4) DNS query logs or NetFlow records from the perimeter showing large outbound transfers to non-standard destinations from HR/payroll system hosts.

Step 3: Eradication — Rotate all credentials for HR, payroll, and document management systems, prioritizing service accounts and administrative accounts (D3-CRO: Credential Rotation). Enforce MFA on all administrative and remote access paths to HR/payroll platforms (D3-MFA; CIS 6.3, 6.4, 6.5; NIST AC-17). Review and tighten access control lists on document repositories to enforce least privilege (NIST AC-6; CIS 3.3). Audit and revoke any dormant or over-privileged accounts (CIS 5.3, 5.4; NIST AC-2). Disable or restrict public-facing application endpoints not required for operations (consistent with T1190 mitigation).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), NIST AC-17 (Remote Access), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5

(Require MFA for Administrative Access), CIS 3.3 (Configure Data Access Control Lists)

Compensating: For credential rotation without an enterprise PAM tool: use the Snowflake command `ALTER USER SET PASSWORD='' MUST_CHANGE_PASSWORD=TRUE;` and immediately reset all Snowflake STORAGE INTEGRATION and NOTIFICATION INTEGRATION credentials. For PeopleSoft, reset the PS application server domain password via `psadmin -p changepwd` and rotate the database connect ID in the PeopleSoft configuration. For MFA enforcement without enterprise SSO, enable Snowflake MFA via `ALTER USER SET MFA_ENABLED=TRUE;` and Salesforce My Domain MFA enforcement in Setup. For ACL tightening on a Windows document share, use `icacls /reset` followed by explicit grants to required groups only.

Evidence: Before rotating any credential or revoking any account, capture: (1) full memory dump of any PeopleSoft application server process using ProcDump (`procdump.exe -ma dump.dmp`) to preserve in-memory session tokens that may identify the attacker's active session; (2) `netstat -ano` and `Get-NetTCPConnection` output from all HR/payroll application hosts to document any live attacker connections that credential rotation will terminate; (3) current Snowflake session list via `SHOW SESSIONS;` and Salesforce active session list from Setup > Active Sessions — export before revocation destroys visibility; (4) Windows Security Event Log Event ID 4624 (Successful Logon) and 4648 (Logon with Explicit Credentials) from PeopleSoft web server hosts, exported to a preserved log archive before rotation closes the window for attacker session tracing.

Step 4: Recovery — Validate that access control changes are in effect across all HR and payroll system tiers. Confirm audit logging is active and centralized per NIST AU-2, AU-12, and CIS 8.2. Run a privileged account review against your account inventory (CIS 5.1) to confirm no residual unauthorized accounts remain. Monitor for secondary extortion contact, data publication attempts, or downstream credential abuse using identity threat detection tooling. Establish a watch on ShinyHunters' known leak sites for publication of claimed data as the June 16, 2026 deadline approaches.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 8.2 (Collect Audit Logs)

Compensating: Without enterprise identity threat detection tooling, configure free compensating controls: (1) Deploy Sysmon with Event ID 4648 monitoring via a Sigma rule to detect credential reuse from new source IPs against HR systems; (2) Use Snowflake's built-in `SNOWFLAKE.ACCOUNT_USAGE.LOGIN_HISTORY` on a daily cron-triggered query to alert on new client IPs or user agents not seen in the prior 30-day baseline; (3) For leak site monitoring, set up a free Google Alert or RSS monitor on ShinyHunters' known Telegram channel identifiers and BreachForums post patterns for 'Council of Europe'; (4) Validate audit log centralization by running `auditpol /get /category:*` on Windows HR hosts to confirm all required event categories are actively logging.

Evidence: Recovery validation does not alter live attacker state if eradication is confirmed complete, but log continuity must be verified: confirm that NIST AU-12 audit record generation is active by verifying Snowflake ACCOUNT_USAGE data is flowing (query `SELECT MAX(EVENT_TIMESTAMP) FROM SNOWFLAKE.ACCOUNT_USAGE.LOGIN_HISTORY;` — a stale timestamp indicates logging is broken), and confirm Windows Security Event Log forwarding is active on all HR/payroll hosts by checking Windows Event Forwarding subscription status. Preserve all pre-recovery log exports from Step 3 in a forensically sound, write-protected archive with hash verification (SHA-256) before returning systems to normal operation.

Step 5: Post-Incident — Conduct a gap assessment against NIST AC-6 (Least Privilege), AC-3 (Access Enforcement), and AU-6 (Audit Record Review) to identify control failures that may have permitted bulk data access. Evaluate third-party data-sharing agreements and vendor access controls (NIST AC-20). Implement or validate D3-UAP (User Account Permissions) and D3-LAM (Local Account Monitoring) countermeasures. Review data retention scope — 15-year data exposure suggests retention policy enforcement gaps (CIS 3.4). Brief legal and communications teams on extortion response protocol before the deadline.

NIST Phase: Post Incident

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

Controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), NIST AC-20 (Use Of External Systems), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 3.4 (Enforce Data Retention)

Compensating: Without a GRC platform for gap assessment, conduct the AC-6 least privilege review manually: export all PeopleSoft role assignments from the PSROLEUSER table (`SELECT ROLEUSER, ROLENAME FROM PSROLEUSER ORDER BY ROLEUSER;`) and compare against a current employee roster to identify over-provisioned or orphaned accounts. For data retention enforcement, audit Snowflake TIME_TRAVEL and FAIL_SAFE retention settings per table (`SHOW TABLES IN DATABASE ;` and review RETENTION_TIME column) to identify where 15-year-old records may have persisted beyond policy. Document all findings in a post-incident report referencing the specific ShinyHunters extortion timeline, the June 16, 2026 deadline, and the categories of exposed data (HR, payroll, medical, financial) for regulatory breach notification analysis.

Evidence: No live state alteration in this phase — all volatile evidence should already be preserved from Steps 1–4. For post-incident reconstruction, ensure the following artifacts are included in the forensic record: (1) final preserved exports of Snowflake QUERY_HISTORY and ACCESS_HISTORY for the full suspected compromise window; (2) PeopleSoft PSACCESSLOG and PSAUDIT table exports covering the 15-year data scope to establish what was accessible; (3) timeline of ShinyHunters' public claims, BreachForums post metadata, and any extortion communications received, preserved with hash verification; (4) ACL snapshots taken before and after Step 3 remediation to document the gap state for regulatory reporting. Flag for legal: the exposure of medical and financial records for 10,000+ staff across multiple jurisdictions likely triggers GDPR Article 33 breach notification obligations within 72 hours of confirmation.

Detection Guidance

Focus detection on bulk data access and exfiltration patterns rather than a single exploit signature, as no CVE anchors this incident. Key signals: (1) Anomalous authentication events against HR and payroll platforms using valid accounts during off-hours (T1078), query identity provider logs and application authentication logs for unusual source IPs or user agents against PeopleSoft, Salesforce, or equivalent HR platforms. (2) Mass document retrieval or export events from document management or cloud storage systems (T1213, T1530), look for single accounts pulling >100 documents in a session, or export jobs not initiated through standard workflows. (3) Large outbound data transfers, especially to cloud storage or code repositories (T1041, T1567.002), DLP or proxy logs showing multi-GB outbound transfers to non-standard destinations are a primary indicator. (4) Privilege escalation events preceding bulk access (CWE-269, T1078), review role-change or privilege-grant events in the 72-hour window before any anomalous bulk access. No confirmed IOCs (file hashes, IPs, domains) have been publicly released for this specific incident. IOC table reflects this gap. Behavioral detection via UEBA or similar tooling aligned with the above patterns is the most actionable path.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`no confirmed IOCs publicly released for this incident`	ShinyHunters has not published technical indicators for the Council of Europe campaign as of the discovery date; monitor threat intelligence feeds and ShinyHunters-associated leak forums as the June 16, 2026 deadline approaches	LOW

Framework Mappings

MITRE-ATTACK

- **T1567.002** — Exfiltration to Cloud Storage
- **T1078** — Valid Accounts
- **T1213** — Data from Information Repositories
- **T1530** — Data from Cloud Storage
- **T1486** — Data Encrypted for Impact
- **T1041** — Exfiltration Over C2 Channel
- **T1190** — Exploit Public-Facing Application
- **T1657** — Financial Theft

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest

OWASP-TOP10-2021

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

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.312(d)** — Person or Entity Authentication

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control

- **6.3** — Require MFA for Externally-Exposed Applications

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1567.002	Exfiltration to Cloud Storage	Exfiltration
T1078	Valid Accounts	Defense-Evasion
T1213	Data from Information Repositories	Collection
T1530	Data from Cloud Storage	Collection
T1486	Data Encrypted for Impact	Impact
T1041	Exfiltration Over C2 Channel	Exfiltration
T1190	Exploit Public-Facing Application	Initial-Access
T1657	Financial Theft	Impact

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/council-of-europe-in...	T3
ShinyHunters Hit Oracle PeopleSoft and Your Vendors May Already ...	https://blackkite.com/blog/shinyhunters-hit-oracle-peoplesoft-and-y...	T3
ShinyHunters target Oracle PeopleSoft in large-scale data theft ...	https://fieldeffect.com/blog/shinyhunters-oracle-peoplesoft-campaign	T3
ShinyHunters Targets Education Sector with Oracle PeopleSoft Exploit	https://cloud.google.com/blog/topics/threat-intelligence/shinyhunte...	T3

Source	URL	Tier
ShinyHunters and UNC6395: Inside the Salesforce and Salesloft ...	https://www.mitiga.io/blog/shinyhunters-and-unc6395-inside-the-sale...	**T3**

Generated 2026-06-16 07:19 UTC by TJS Security Command Center