TLP:RED THREAT ACTOR · EXECUTIVE BRIEFING

ShinyHunters

Seven Years of Data-Theft Capitalism

From the database bazaar to a federated extortion brand: **3B+ records**, **300+ named victims**, and one alliance reshaping global cybercrime.

ShinyHunters at a glance

The longest-running, most adaptive financially-motivated data-theft group of the past decade.

3B+

RECORDS STOLEN · LIFETIME

Across 7 years and 5 operational eras

3.65 TB

STOLEN FROM CANVAS

~330 institutions defaced May 7; Instructure paid the ransom May 11

5

DISTINCT OPERATIONAL ERAS

Each defined by a new attack surface — not an upgrade of the last

Business model: exfiltrate, extort, leak. Each era refines the same model and applies it one layer higher in the enterprise stack — consumer DBs → cloud warehouses → Salesforce CRM → SaaS supply chain → identity-platform fronts. As of July 2026 ShinyHunters runs multiple concurrent enterprise campaigns — not as a single group, but as a **federated brand**.

Three developments the C-suite must internalize

CRITICAL

The Salesforce Vishing Campaign

Industrial-scale voice-phishing — Google, Cisco, Adidas, Qantas, LVMH, Allianz, Workday, Pandora, Chanel, TransUnion. ShinyHunters claims **1.5B records** from **760 Salesforce tenants** via stolen Drift OAuth tokens.

CRITICAL

The SLH Alliance Federation

August 2025: ShinyHunters + Scattered Spider + LAPSUS$ publicly merge as **Scattered LAPSUS$ Hunters**. Pooled initial access, exfiltration and extortion capability. Brand identity is now plural — and partially impersonated.

HIGH

Education Is a Strategic Target

3.65 TB / 275M Canvas records via a Free-for-Teacher ticket flaw. ~330 portals defaced May 7; ransom paid May 11. Penn, Princeton, Harvard, McGraw Hill, Follett — sector-wide, not isolated.

Five eras, one business model

Each era industrialises the previous era's tradecraft against a higher-leverage attack surface — same model, escalating blast radius.

1 2019–2021

The Database Bazaar

WHAT HAPPENED

Rose on the breach-forum economy. Databases auctioned on RaidForums; harvested creds reused.

WHY IT MATTERS

Built the brand into a tradeable trademark that survived every later takedown.

2 2022–2023

Law-Enforcement Reckoning

WHAT HAPPENED

Raoult arrested 2022, sentenced 2024 (36 mo + $5M). Co-conspirators indicted — ops continued.

WHY IT MATTERS

Decapitation needs a leader. SH never had one — alliance ties were already live.

3 2024

Snowflake Inferno

WHAT HAPPENED

UNC5537 bought infostealer logs, walked into ~165 Snowflake tenants. AT&T paid ~$370K BTC.

WHY IT MATTERS

Broke the one-victim model — one platform under 165 enterprises, parallel extortion.

4 Jun–Aug 2025

Salesforce Vishing

WHAT HAPPENED

Vishing → modified Data Loader → mass exfil. Aug 28: Drift OAuth theft — 760 tenants, 1.5B records.

WHY IT MATTERS

"We have MFA" bypassed by social engineering. Defence shifts to identity and OAuth.

5 Aug 2025–now

SLH Alliance

WHAT HAPPENED

SH + Scattered Spider + LAPSUS$ federate. "Retirement" was performative — Aura, Canvas followed.

WHY IT MATTERS

Brand is plural but unequal — treat attribution as brand, not forensic.

Who is "ShinyHunters" today?

Per HivePro `TA2026107` (April 2026): the name is used by at least three operationally distinct entities. Treat every attribution claim as a marketing assertion to be validated.

ENTITY 1

The Original Cluster

Inside the SLH Alliance

High-end campaigns: Salesforce vishing (Cisco, Adidas, Qantas), Drift/Gainsight OAuth, Salesforce Aura, Canvas/Instructure. Operates the `shinyhunte.rs` DLS and the canonical Tox / BTC negotiation channels.

ENTITY 2

Impersonators

Extortion using the brand

Telegram and dark-web operators using the ShinyHunters name without affiliation. Observed in the May 2025 PowerSchool school-district re-extortion. ShinyHunters publicly denied operating retail sales channels.

ENTITY 3

Data Resellers

No intrusions, just resale

Operators like "DB+ Collector" who do not breach — they aggregate and resell infostealer-log credentials under the umbrella name. Their threat is credential exposure, not direct system compromise.

IMPLICATION: Paying one "ShinyHunters" extortion does not prevent another. The brand is plural — extortion liability is **per-claim, not per-actor**.

Salesforce breach — five-step tradecraft loop

Each step has discrete defensive controls — and a different team accountable for them.

1

Identity Acquisition

Vishing to help desk; IT-impersonation calls; victim-branded credential portals; real-time MFA relay; infostealer log markets.

›

2

Persistence

Register attacker MFA device; delete "method enrolled" emails (ToogleBox Recall); authorize malicious Connected Apps.

›

3

Lateral Movement

SSO session pivots Salesforce → M365 → SharePoint → Slack. Search for `confidential, internal, proposal, vpn`.

›

4

Exfiltration

Modified Salesforce Data Loader; PowerShell-driven SharePoint bulk downloads; OAuth token-stuffed API extraction.

›

5

Extortion

72-hour BTC timer via Tox; DLS publication; SMS harassment; DDoS amplification; private dataset sale up to $1M.

KEY: No malware executes on an endpoint in steps 1–4. **EDR has zero defensive value** against this chain — the high-leverage controls are identity-side and SaaS-audit-side, not endpoint-side.

CVEs in scope — direct & alliance-partner

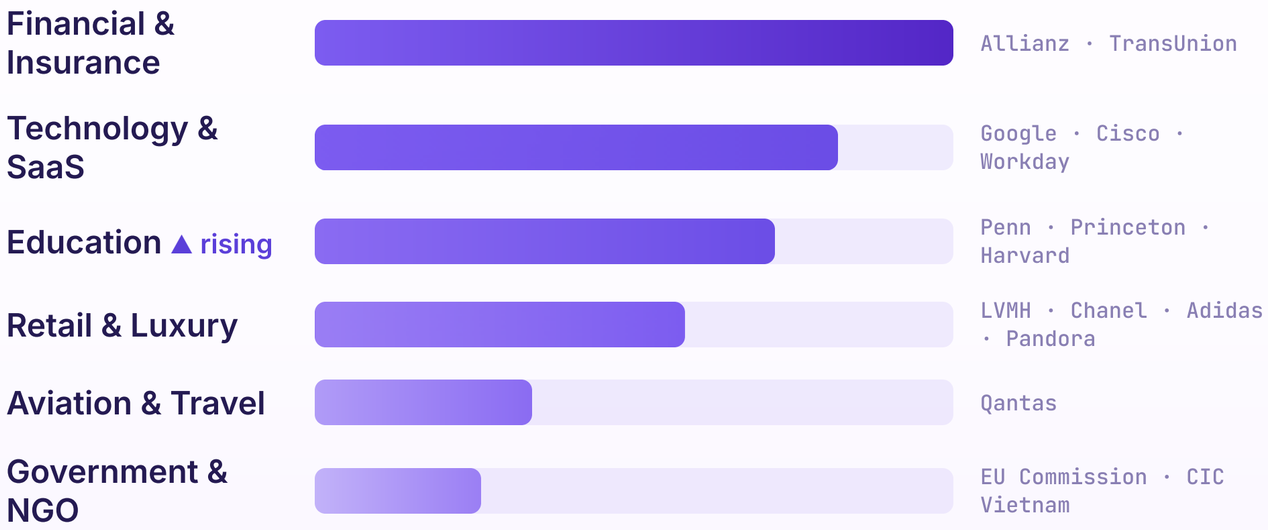
ShinyHunters is identity-first; CVEs are minor. Most of the attack surface is SaaS integrations and OAuth abuse — not patchable bugs.

DIRECTLY EXPLOITED BY SHINYHUNTERS & SLH PARTNERS

CVE	PRODUCT	CVSS	USE
CVE-2025-31324	SAP NetWeaver — unrestricted file upload	10.0	SLH publicly claimed exploit
CVE-2025-61882	Oracle E-Business Suite (BI Publisher)	9.8	SLH leaked PoC Oct 2025; Cl0p mass exploit
CVE-2021-35587	Oracle Access Manager	9.8	"Yukari" persona — Oracle 12c data theft
CVE-2026-35273	Oracle PeopleSoft Enterprise PeopleTools	9.8	Unauthenticated RCE for initial access
no CVE	Salesforce Aura / Experience Cloud misconfig	–	Mar 2026 — ~400 companies
no CVE	Salesloft-Drift OAuth token theft	–	TruffleHog → 760 SF tenants → 1.5B records
no CVE	Gainsight Salesforce integration OAuth abuse	–	Nov 2025 — 285 SF instances

Where ShinyHunters has hit hardest

Relative concentration of named victims across SLH-era operations, by sector.



WHAT THIS TELLS US

Financial services leads

Salesforce CRM penetration is highest — UNC6040 hits where the data is.

Tech & SaaS clusters

Around the Drift/Gainsight cascade — vendors breached through their customers' integrations.

Education is the newest escalation

Most concentrated — Penn → Harvard → Princeton → Canvas in 8 months.

IOC landscape

High-level inventory. The complete IOC corpus — with full payment & negotiation indicators — is in the HiveForce Labs advisories on Oracle EBS, PeopleSoft, and ShinyHunters brand-hijack.

26
IPV4 ADDRESSES
Across UNC6661 / UNC6671 / SLH clusters

22
PHISHING DOMAINS
`<company>sso`, `<company>okta`

95+
SHA256 HASHES
LummaC2, StealC, Vidar, RedLine, Meduza, Rhadamanthys

6
NEGOTIATION CHANNELS
Tox, Tutanota, OnionMail, BTC, XMR, .onion DLS

PRIORITY DETECTION TARGETS

- **Phishing domain pattern:** `<company>sso.com`, `<company>okta.com`, `<company>internal.com` — via NICENIC or Tucows.
- **Exchange / SharePoint:** deletes of "new MFA" / "method enrolled" emails; PowerShell UA downloading >50 files in 5 min.
- **OAuth grant anomaly:** ToogleBox Recall auth in Google Workspace; new Salesforce Connected App approvals outside change windows.
- **Network:** auth from Mullvad, Oxylabs, NetNut, 9Proxy, Infatica, nsocks — **hunt, do not blindly block**.

MITRE ATT&CK — operational hotspots

Heat shows where SLH operators spend the most time.

Initial Access — HIGH

T1566.004 Spearphishing Voice

T1078 Valid Accounts

T1195 Supply Chain Compromise

Credential Access — HIGH

T1111 MFA Interception

T1528 Steal App Access Token

T1539 Steal Web Session Cookie

Persistence — HIGH

T1098.005 Device Registration

T1136.003 Cloud Account

Defense Evasion — MEDIUM

T1550.001 App Access Token Reuse

T1578.005 Modify Cloud Compute

Collection — HIGH

T1213 Data from Info Repos

T1119 Automated Collection

Exfiltration — HIGH

T1567.002 Exfil to Cloud Storage

T1041 Exfil over C2

T1020 Automated Exfiltration

Command & Control — MEDIUM

T1071.001 Web Protocols

T1090.003 Multi-hop Proxy

Impact — HIGH

T1657 Financial Theft

T1498 Network DoS

The next 90 days

Where the SLH alliance is most likely to escalate — based on tradecraft maturity, attack-surface migration, and recently-claimed access.

HIGH LIKELIHOOD

Education-sector escalation continues

A confirmed payday on a 3.65 TB exfil invites pressure on Blackboard, D2L and Schoology customers, direct K-12 district extortion, donor/alumni lifts at more Ivies, and follow-on phishing against 9,000 Canvas institutions.

HIGH LIKELIHOOD

More Salesforce-AppExchange supply-chain hits

Drift and Gainsight set the playbook. Any AppExchange integration with broad OAuth scopes — analytics, AI assistants, marketing-attribution — is a viable vector. Expect another large OAuth cascade by Q3.

MEDIUM LIKELIHOOD

ShinySp1d3r RaaS launches operationally

The teased VMware ESXi ransomware would move SLH from pure data-theft into encryption-enabled double extortion. Initial victims likely in manufacturing or healthcare.

MEDIUM LIKELIHOOD

Government / NGO extortion expansion

EU Commission and CIC Vietnam show willingness to hit state-affiliated targets. Expect additional EU agencies, mid-tier national governments, and large NGOs — testing the political response calculus.

Four pillars — ordered by leverage, not familiarity

Derived from HivePro TA2026107, the Mandiant Jan 2026 hardening guide, and SLH post-incident response patterns.

1

Phishing-Resistant MFA

FIDO2 keys or passkeys for all workforce — mandatory for SSO admins. Push, SMS and TOTP are trivially captured by vishing. Hardware-bound credentials cannot be relayed.

2

SaaS Integration Governance

Daily OAuth-token audit. Allowlist Connected Apps. Remove mass-export from non-admins. Define trusted IP ranges. Rotate API keys in GitHub, GitLab, Jira, Azure DevOps.

3

Post-Compromise Detection

Alert on ToogleBox Recall auth, deletion of "MFA enrolled" emails, PowerShell SharePoint bulk downloads, Data Loader exports from untrusted IPs, Okta admin roles from anonymized IPs.

4

24-Hour Patch SLA on Internet-Facing Apps

Prioritize `CVE-2025-31324` (SAP NetWeaver), `CVE-2025-61882` (Oracle EBS), `CVE-2021-35587` (Oracle Access Manager).

Leveraging the Hive Pro platform

Every row is actionable within an hour of read. Subscribe once, ingest continuously.

WORKFLOW	ACTION
Threat Actor Search	Subscribe to ShinyHunters, Scattered Spider, LAPSUS$ — auto-alert on new IOCs / TTPs.
Vulnerability Module	Track & prioritize `CVE-2025-31324, 2025-61882, 2021-35587, 2026-35273`.
Malware Library	Monitor LummaC2, StealC, Vidar, RedLine, Meduza, Rhadamanthys — the infostealer pipeline feeding SLH access.
IOC Ingestion	Auto-import IOCs from advisories `TA2025307, TA2026107, TA2026165` into SIEM, EDR, firewall, SaaS-audit telemetry.
Attack Surface Module	Discover external exposure and map each exposed asset to known, operationally-exploited CVEs.
Campaign Tracking	Subscribe to active campaigns: Aura misconfig, SSO-vishing, Drift/Gainsight OAuth abuse, third-party SaaS supply-chain.

CLOSING

Are you exposed to ShinyHunters?

Identify ShinyHunters / SLH-alliance exposure across your SaaS estate, identity stack, and external attack surface — in hours, not weeks.

Sign up for a free exposure report →

Subscribe to the Weekly Threat Digest

SCAN TO GET YOUR REPORT

hivepro.com/threat-advisory