

Latest Cyber Threat Intelligence & Security Insights

Archived: 2026-07-28 02:01:03 UTC

The Rise of the Federated Cybercriminal Brand

The cyber threat landscape has witnessed the emergence of the **Scattered LAPSUS\$ Hunters (SLSH)**, a highly effective threat actor collective formalized in 2025. SLSH represents a dangerous fusion of methodologies and personnel from **Scattered Spider** (UNC3944/OCTOPUS), **ShinyHunters** (UNC6040/UNC6240), and surviving LAPSUS\$-style groups.

Through direct access to one of their latest private Telegram channels (349 members, active “part 7” spin-off) and cross-correlation with reporting from KrebsOnSecurity, Hudson Rock, Mandiant, Trustwave SpiderLabs, Palo Alto Unit 42, Picus Security, S2W TALON, and ReliaQuest, we have produced a consolidated view of the group’s current leadership, infrastructure, TTPs, and indicators of compromise.

Operating at scale despite coordinated disruption attempts, SLSH leverages a blend of sophisticated social engineering, targeted insider recruitment, and high-impact data extortion. Reporting confirms their involvement in over **1,500 breaches** across the SaaS, retail, and telecom sectors, with successful extortions documented at **\$370,000+**. This briefing consolidates the group's current structure, infrastructure, and Tactics, Techniques, and Procedures (TTPs) as of November 2025.

Current Leadership and Operational Personas (November 2025)

SLSH maintains a dynamic and evasive command structure, utilizing distinct personas to coordinate operations and execute psychological warfare.

Our FalconFeeds dataset aligns closely with KrebsOnSecurity's November 26 exposure of "Rey" as 15-year-old Saif Al-Din Khader (Amman, Jordan), a key SLSH admin cooperating with EU law enforcement since June 2025, and S2W TALON's November 25 report on the group's core personas.

Highlights

Rey ★

- Operations coordinator
- Variable (pink “R” avatar)
- Previously @jolt30n → Rey (Oct 2025). Linked to +98 919 362 xxxx (Iran MCI SIM, active Oct–Nov 2025; potential cutout per ReliaQuest Iranian nexus analysis). Frequently posts PoCs and insider recruitment calls, tying to Picus' August 31 "v4.0" channel targeting enterprise moles.

famous celebrity Sex / Sevy

- Psychological ops & evasion
- 7327440053
- 18-month username rotation documented (May 2024 – Nov 2025). Notable handles: @KAngel_uwu, @sevykitten, @ISEEITILIKEITIWANTITIG0TITxDUwU, @barbie, current @kAngel_uwu with bio “famous celebrity”. Directly posted media in the monitored channel; evasion patterns match Hudson Rock stealer logs and Krebs' Com ecosystem ties.

Rose

- Automated vetting/greeter bot
- Welcomes new members by username, scans profiles, auto-bans non-compliant users. Used for rapid insider vetting and lurker detection, consistent with Trustwave's opsec analysis of SLH's distributed trust model.

Key Indicators of Compromise (IOCs) and Infrastructure

IOCs from our scrapes correlate with Mandiant's October 2025 victim shaming blog tracking (e.g., Red Hat GitLab 570GB exfil) and Socradar's November 21 Gainsight supply-chain IOCs.

Telegram Infrastructure

Invite proxy: t.me/comefacecediswood (obfuscation per Trustwave's 16+ respawn cycle since August 8, 2025).809b8c035f41

Current channel title fragment: “Scattered LAPSUS\$ hunters part” (exact ID/hash available under NDA).

Previous iterations: “scattered LAPSUS\$ hunters 4.0”, “The Com HQ v16”, etc. (16 documented respawns since August 8, 2025).

Gift/Stars Laundering Network (UID 7327440053)

- 8042142303
- 6524181273
- 7082816478
- 5227369252
- 7664921784
- 1002845113
- 7739896501
- 7300061657
- 7336399295
- 5905091787

Used for low-friction affiliate payouts and channel boosts, aligning with Picus' RaaS funding observations.

Telephone Number

+98 919 362 xxxx – attributed to Rey (Tehran prefix, recovered from 2025 MCI breach datasets; echoes ReliaQuest's Iran-SS infrastructure links).

Consolidated TTP Matrix (MITRE ATT&CK v15)

TTPs draw from Picus Security's October 20 supergroup analysis (e.g., Scattered Spider's vishing + ShinyHunters' exfil) and Trustwave's November 7 federated brand breakdown, with our FalconFeeds logs confirming OAuth persistence in Gainsight claims.

Reconnaissance

- T1589.002 / T1593
- LinkedIn scraping + employee directory enumeration for helpdesk & super-admin targeting; correlates with ReliaQuest's 12% financial sector domain spike since July 2025.

Initial Access

- T1566.004 (Vishing)
- Helpdesk impersonation → MFA fatigue / OAuth consent phishing; Mandiant ties to May-Sep 2025 Salesforce campaigns.

Initial Access

- T1078.002 (Valid Accounts)
- Purchase or groom insiders for domain-admin / Okta super-admin credentials; Picus notes August 31 recruitment in "v4.0" channel.efeb72

Persistence

- T1134 / T1528
- OAuth token theft & refresh-token manipulation (Salesforce, Microsoft 365, GitHub); Obsidian confirms 10x blast radius in Salesloft-Drift supply chain.

Defense Evasion

- T1562.001
- Disable EDR telemetry, rapid Telegram channel rotation; Trustwave documents 16 nukes/rebirths as psyop resilience.

Credential Access

- T1003.002 / T1110.004
- ntds.dit dumps, OST/PST exfiltration; Hudson Rock stealer logs link to Sevy personas.

Discovery

- T1087.002 / T1069
- Active Directory & Azure AD enumeration post-compromise; eSecurity Planet maps to GitHub repo scans in Salesloft breach.

Lateral Movement

- T1570
- RDP, AnyDesk, FleetDeck, privileged VPN profiles; Dark Reading notes Mullvad VPN obfuscation in 2025 attacks.

Exfiltration

- T1567.002
- Cloud API exfiltration (Salesforce connected apps, SharePoint, GitHub repos); Krebs details 570GB Red Hat GitLab dump.

Impact

- T1486 + Extortion
- Double-extortion model (leak site + direct negotiation); emerging ESXi ransomware beta “SHINYSP1D3R” per BleepingComputer and S2W.

Victimology and Noteworthy Activity (Aug–Nov 2025)

SLSH actively targets organizations with large datasets and crucial supply-chain access.

- Correlates with Krebs' October 2025 spree (e.g., Oracle CVE-2025-61882 exploit leak) and Socradar's November 21 Gainsight advisory (Mandiant forensics confirming external app compromise).
- LVMH / Gucci (160M+ records; ShinyHunters exfil per Mandiant).
- Qantas (extortion with injunction dodge; ReliaQuest aviation targeting).
- CrowdStrike / Gainsight (supply-chain access attempts, \$25K–\$30K insider bribes; Unit 42 IOCs).
- Red Hat GitLab (570GB source code; Crimson Collective collab per Trustwave).
- Multiple Fortune-500 SaaS providers via OAuth abuse (ongoing claims on Bling Libra DLS; 1B+ records per Rescana).

Conclusion

SLSH has emerged as one of the most adaptive and resilient threat actor collectives of 2025, combining the social-engineering strengths of Scattered Spider, the data-theft capabilities of ShinyHunters, and the aggressive extortion model of LAPSUS\$. Their decentralized structure, evolving personas, and focus on identity abuse allow them to bypass traditional security controls and scale attacks across SaaS, telecom, and supply-chain environments. Effective defense requires prioritizing identity hardening, monitoring OAuth and cloud integrations, and strengthening insider-threat detection. As SLSH continues to evolve, organizations must adapt quickly to counter a threat model built on speed, deception, and persistent access abuse.

Source: <https://falconfeeds.io/blogs/scattered-lapsus-hunters-slsh-threat-intelligence-2025/>