ZEROFOX INTELLIGENCE

Flash

Scattered Lapsus$ Hunters Announce Temporary Dissolution

F-2026-10-15a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Threat Actor, Data Breach

October 15, 2025

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 7:00 AM (EDT) on October 15, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Scattered Lapsus$ Hunters Announce Temporary Dissolution

| Key Findings

- Threat collective Scattered Lapsus$ Hunters (SLSH) posted on its Telegram channel on October 11, 2025, that it was ceasing activities until 2026, likely in an effort to reduce law enforcement (LE) scrutiny while retooling and figuring out the group's next steps.
- SLSH is touting the launch of an EaaS campaign—a growing trend offered by threat collectives—on its Telegram channel. This announcement was posted several hours before the one indicating SLSH was dissolving and is almost certainly indicative of the group's intent to remain a prominent threat collective in the cybercrime landscape throughout 2026 and gain further market share of potential affiliates.
- The announcement to temporarily dissolve is almost certainly due to increased scrutiny by LE elements. It is very likely SLSH will use the pause to review its operational security and seek ways to avoid further LE disruptions.

Details

Threat collective SLSH posted on its Telegram channel on October 11, 2025, that it was ceasing activities until 2026,[1] likely in an effort to reduce LE scrutiny while retooling and figuring out the group's next steps. SLSH began operations in August 2025 and has most recently claimed responsibility for an extortion campaign against Salesforce.

- In the same post, SLSH claimed it would be concentrating its efforts on targeting U.S. government employees—specifically those working for the U.S. Federal Bureau of Investigations (FBI) and the National Security Agency (NSA)—almost certainly in retaliation for the FBI's seizure of the popular English-language deep and dark web forum BreachForums.
- The FBI's seizure of BreachForums disrupted a major leak extortion site used by SLSH to highlight its wave of attacks on Salesforce customers.[2]
- SLSH previously announced in September that it would disband before reappearing. On September 11, 2025, SLSH announced on its public Telegram channel that it was ceasing operations; however, the group reappeared three days later, as reported by ZeroFox.[3][4]

SLSH is touting the launch of an EaaS campaign—a growing trend offered by threat collectives—on its Telegram channel. This announcement was posted several hours before the one indicating SLSH was dissolving and is almost certainly indicative of the group's intent to remain a prominent threat collective in the cybercrime landscape throughout 2026 and gain further market share of potential affiliates.

---

1 hXXps://databreach[.]com/news/29-fear-and-loathing-in-the-comm---scattered-lapsus-hunters-turn-extortion-into-a-service

2 hXXps://www.bleepingcomputer[.]com/news/security/fbi-takes-down-breachforums-portal-used-for-salesforce-extortion/

3 hXXps://t[.]me/sctt3rd/1601

4 https://www.zerofox.com/intelligence/flash-report-prominent-threat-collective-announces-disbandment/

- On August 8, a new account surfaced on Telegram named “scattered lapsu$ hunters - The Com HQ SCATTERED SP1D3R HUNTERS”. The channel was launched by individuals claiming to be part of the prominent cybercrime collectives Scattered Spider, Lapsus$, and ShinyHunters.
- On August 11, the scattered lapsu$ hunters - The Com HQ SCATTERED SP1D3R HUNTERS channel was banned from Telegram; however, the group quickly migrated to a new backup channel. In its brief four-day lifespan, posts on the scattered lapsu$ hunters - The Com HQ SCATTERED SP1D3R HUNTERS channel resembled the types of activity displayed within the Telegram channels operated by Scattered Spider, Lapsus$, and ShinyHunters.

The announcement to temporarily dissolve is almost certainly due to increased scrutiny by LE elements. It is very likely SLSH will use the pause to review its operational security and seek ways to avoid further LE disruptions. Although SLSH has indicated that it will return in 2026, there is a likely chance that the group will resurface over the coming weeks in order to pursue its intended targeting of the FBI and NSA outlined in the October 11 post. Furthermore, there is a roughly even chance that SLSH will return before 2026 to continue its other observed activities, such as data breaches and data leaks.

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** TLP:AMBER+STRICT restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%