ZEROFOX INTELLIGENCE

Flash

Scattered Lapsus$ Hunters Announce Return

F-2025-11-27a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Data Breach, Threat Actor, Malware

November 27, 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 (EST) on November 27, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Scattered Lapsus$ Hunters Announce Return

| Key Findings

- On November 24, 2025, ZeroFox observed that the threat collective "Scattered Lapsus$ Hunters" (SLSH) had seemingly resumed activity through a new Telegram channel after nearly a month of silence.
- Multiple posts on the Telegram channel suggest that SLSH is offering financial incentives and actively recruiting insiders who can provide initial access to corporate networks.
- Recent messages on the channel likely indicate an escalation of border threats of disruption compared to previous publications.
- SLSH's recent activity on Telegram almost certainly indicates clear intent to continue and likely escalate its previously observed operations, such as conducting data breaches and data leaks, publicly exposing corporations, and actively recruiting insiders.

Details

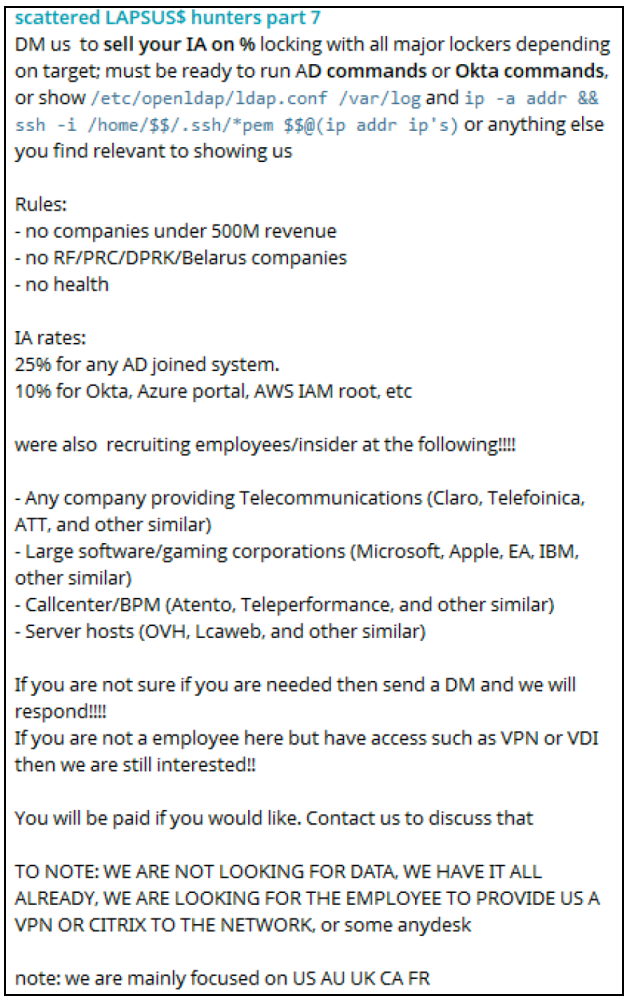
On November 24, 2025, ZeroFox observed that the SLSH threat collective had seemingly resumed activity through a new Telegram channel (hXXps://t[.]me/smokinmandiant) after nearly a month of silence.

- On November 19, 2025, reports surfaced of the emergence of an in-development build of a new RaaS platform called "ShinySp1d3r".[1] The new RaaS build is the result of a collaboration between notorious threat collectives "ShinyHunters", "Scattered Spider", and "Lapsus$".
- 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 scrutiny while retooling and figuring out its next steps. SLSH began operations in August 2025 and has most recently claimed responsibility for an extortion campaign against Salesforce.

Multiple posts on the Telegram channel suggest that SLSH is offering financial incentives and actively recruiting insiders who can provide initial access to corporate networks. SLSH is almost certainly seeking access that enables the execution of administrative commands, the retrieval of configuration files, or the establishment of remote connectivity via a Virtual Private Network (VPN), Citrix, or similar secure-access technologies.

- SLSH stated in the channel that there are several criteria in place for eligible insiders; workers at companies with revenue of under USD 500 million; those at organizations in Russia (RF), People's Republic of China (PRC), Democratic People's Republic of Korea (DPRK), and Belarus; and those in the healthcare sector will not be eligible.
- SLSH commented that its recruitment focus includes telecommunications providers, large software and gaming companies, global call center operators, and major server-hosting providers. SLSH likely wants to choose these actors because they offer significant access and leverage to amplify its attacks and campaigns.

[1] https://www.zerofox.com/intelligence/flash-report-powerful-new-raas-from-scattered-lapsus-hunters/


scattered LAPSUS$ hunters part 7
DM us to **sell your IA on %** locking with all major lockers depending on target; must be ready to run A**D commands** or **Okta commands**, or show `/etc/openldap/ldap.conf /var/log` and `ip -a addr && ssh -i /home/$$/.ssh/*pem $$@(ip addr ip's)` or anything else you find relevant to showing us

Rules:
- no companies under 500M revenue
- no RF/PRC/DPRK/Belarus companies
- no health

IA rates:
25% for any AD joined system.
10% for Okta, Azure portal, AWS IAM root, etc

were also recruiting employees/insider at the following!!!!

- Any company providing Telecommunications (Claro, Telefoinica, ATT, and other similar)
- Large software/gaming corporations (Microsoft, Apple, EA, IBM, other similar)
- Callcenter/BPM (Atento, Teleperformance, and other similar)
- Server hosts (OVH, Lcaweb, and other similar)

If you are not sure if you are needed then send a DM and we will respond!!!!
If you are not a employee here but have access such as VPN or VDI then we are still interested!!

You will be paid if you would like. Contact us to discuss that

TO NOTE: WE ARE NOT LOOKING FOR DATA, WE HAVE IT ALL ALREADY, WE ARE LOOKING FOR THE EMPLOYEE TO PROVIDE US A VPN OR CITRIX TO THE NETWORK, or some anydesk

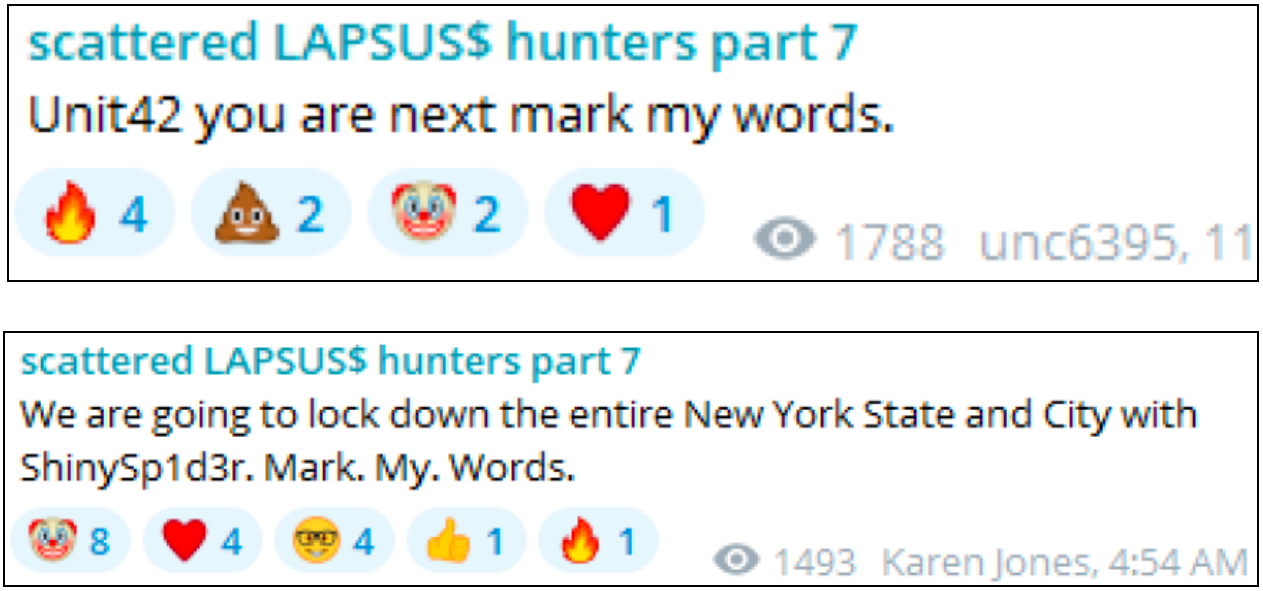
note: we are mainly focused on US AU UK CA FR

Recruitment post on new SLSH Telegram channel

Source: ZeroFox Intelligence

Recent messages on the channel likely indicate an escalation of border threats of disruption compared to previous publications. For example, in one post, SLSH expressed the intent to “lock down” the state of New York by using its newly developed ShinySp1d3r ransomware, which is a newly observed threat. SLSH’s recent messages also publicly name multiple intended targets such as CrowdStrike, Unit 42, and CrunchLabs, a trend that ZeroFox has previously observed.

- Though such statements are likely exaggerated for publicity and intimidation, they contribute to SLSH’s aggressive messaging campaigns and declared willingness to target critical infrastructure.

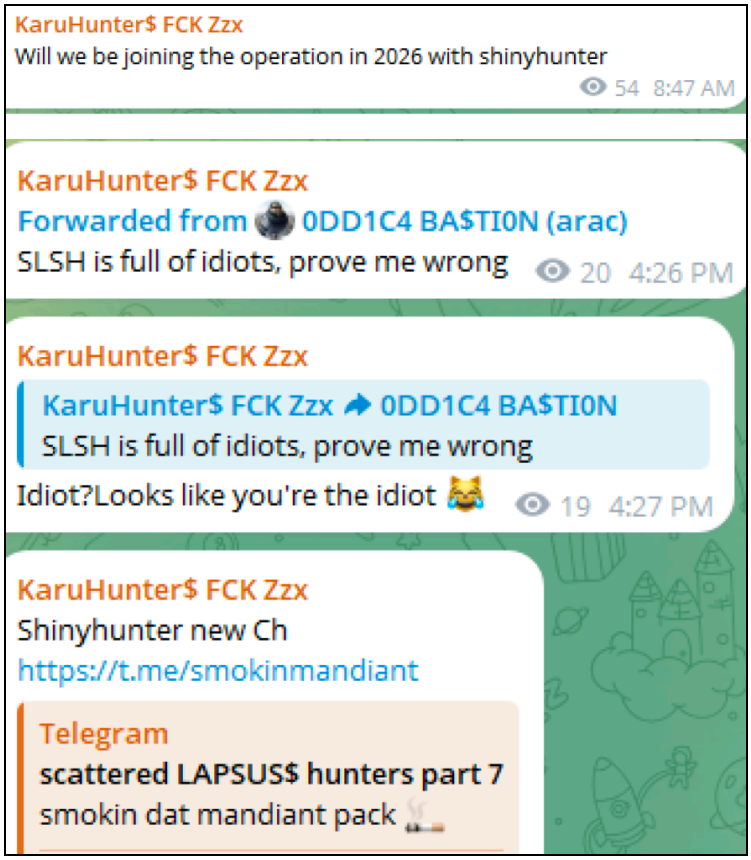


Messages on new SLSH Telegram channel

Source: ZeroFox Intelligence

Notably, ZeroFox observed the threat actor "KaruHunter$ FCK ZZx" promoting SLSH's newly shared Telegram channel link, likely indicating a developing alliance between the two groups. This activity aligns with an earlier post by KaruHunter$ FCK ZZx on November 15, 2025—which stated, "Will we be joining the operation in 2026 with shinyhunter"—further suggesting potential collaborative intent.

- KaruHunters is a reputable threat actor who frequently posts on the dark web forum DarkForums and is known for multiple breaches targeting governments, corporations, and private targets worldwide.



KaruHunter$ FCK ZZx promoting the new SLSH Telegram channel

Source: ZeroFox Intelligence

SLSH's recent activity on Telegram almost certainly indicates clear intent to continue and likely escalate its previously observed operations, such as conducting data breaches and data leaks, publicly exposing corporations, and actively recruiting insiders. Although initially expected to resurface in 2026—as per the group's messaging—it is very likely that SLSH will continue operations in the coming weeks. SLSH will almost certainly target organizations based in the United States and Europe, while also focusing its recruitment efforts in Australia, Canada, and France. The geographical locations of these potential recruits is very likely to be perceived by the group as the most financially lucrative while also having the potential to cause the most disruption and gain the most exposure.

Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Implement secure password policies, phishing-resistant multi-factor authentication (MFA), and unique credentials.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in deep and dark web (DDW) forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).

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%