ZEROFOX INTELLIGENCE

Flash

Powerful New RaaS from Scattered Lapsus$ Hunters

F-2025-11-21a

Classification: TLP:CLEAR

Criticality: Low Impact

Intelligence Requirements: Ransomware, Malware, Threat Actor

November 21, 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 12:00 PM (EST) on November 21, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Powerful New RaaS from Scattered Lapsus$ Hunters

| Key Findings

- On November 19, 2025, reports surfaced of the emergence of an in-development build of new ransomware-as-a-service (RaaS) platform "ShinySp1d3r". The new RaaS build is the result of a collaboration between notorious ransomware and digital extortion (R&DE) collectives Scattered Spider, Lapsus$, and ShinyHunters.
- The threat actors, known collectively as Scattered Lapsus$ Hunters (SLSH), have been responsible for at least 51 cyberattacks over the past year as both individual groups and as a collective.
- While the ShinySp1d3r encryptor has some features common to other encryptors, it also boasts features that have never been seen before in the RaaS space.
- The development of ShinySp1d3r represents a leap in capability for SLSH and suggests a successful merger into a fully functional collective.

Details

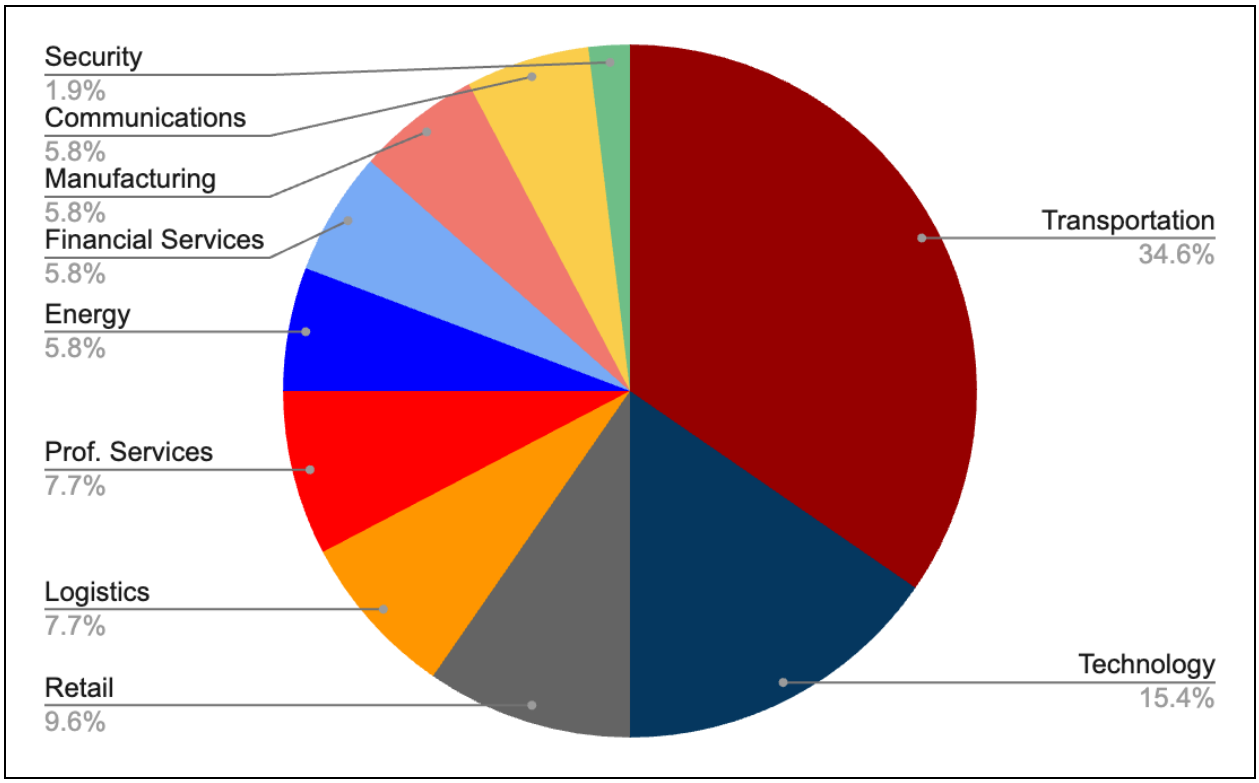
On November 19, 2025, reports surfaced of the emergence of an in-development build of a new RaaS platform called ShinySp1d3r. The new RaaS build is the result of a collaboration between notorious threat collectives Shiny Hunters, Scattered Spider, and Lapsus$.

- On August 8, 2025, a new account named "scattered lapsu$ hunters - The Com HQ SCATTERED SP1D3R HUNTERS" surfaced on Telegram. The channel was launched by individuals claiming to be part of the prominent cybercrime collectives Scattered Spider, Lapsus$, and ShinyHunters.
- On September 11, 2025, prominent threat collective SLSH announced on its public Telegram channel that it was ceasing operations.[1] The message also appeared on the homepage of breachforums[.]hn, with a link to the collective's Telegram page.

The three threat collectives in this endeavor have typically used ransomware encryption from other, more established groups such as ALPHV/BlackCat and Qilin. However, the newly established collective is now creating its own operation, likely in an effort to increase profits by eliminating the sharing of ransoms with platform providers.

ZeroFox has observed that SLSH has been responsible for at least 51 cyberattacks over the past 12 months as both individual groups and as a collective. While these collectives have targeted several industries, transportation and technology account for 50 percent.

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



SLSH's attacks by industry over the past 12 months

Source: ZeroFox Intelligence

The sample of the new ShinySp1d3r RaaS uploaded to the security website VirusTotal is likely built from scratch rather than using leaked code from other encryptors.[2] This development demonstrates that SLSH has made a capability leap that will almost certainly lead to more attacks using the new RaaS in the near future.

While the ShinySp1d3r encryptor has some features common to other encryptors, it also boasts features that have never been seen before in the RaaS space. These include:

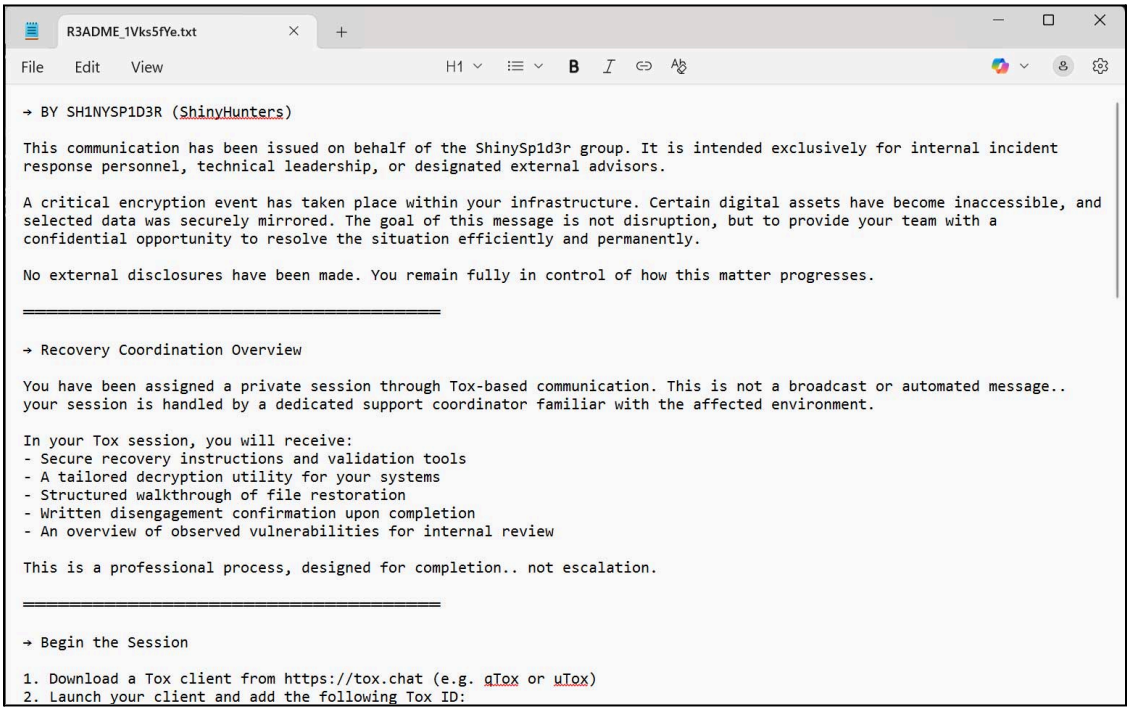
- Hooking the EtwEventWrite function to prevent Windows Event Viewer logging.[3]
- Terminating processes that keep files open—which would normally prevent encryption—by iterating over processes before killing them.

[2] hXXps://www.virustotal[.]com/gui/file/3bf53cddf7eb98d9cb94f9aa9f36c211a464e2c1b278f091d6026003050281de

[3] hXXps://hackyourmom[.]com/en/novyny/shinyhunters-stvoryly-novyj-potuzhnyj-raas-detali-majbutnih-atak-uzhe-vidomi/

- Filling free space in a drive by writing random data contained in a .tmp file, likely to overwrite any deleted files—making them difficult, if not impossible, to recover.
- The ability to propagate to other devices in a network, create its own service to run malware, then initiate the malware, and finally generate a startup script—all contained within the encryptor itself.

Every folder on an encrypted device reportedly contains a ransom note explaining what has happened to the victim's files, as well as instructions on how to negotiate and a Tox address for communications.[4] The ransom note will also reportedly include a link to a TOR data leak site; however, the sample version of ShinySp1d3r currently contains an invalid .onion URL.



Ransom note from ShinySp1d3r

Source: hXXps://www.bleepingcomputer[.]com/news/security/meet-shinysp1d3r-new-ransomware-as-a-service-created-by-shinyhunters/

4 hXXps://www.bleepingcomputer[.]com/news/security/meet-shinysp1d3r-new-ransomware-as-a-service-created-by-shinyhunters/

Analyst Commentary

The development of ShinySp1d3r represents a leap in capability for SLSH. The ability to develop its own ransomware encryptor likely indicates a step up in technological capabilities and further suggests a successful completion of its merger into a larger collective.

The creation of a standalone ransomware encryptor, developed in this instance by SLSH, will almost certainly give the collective a secure platform from which to conduct sophisticated R&DE attacks against organizations across the spectrum of industries—especially those in North America and Europe, which are the constituent groups' most frequently targeted locations.

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%