ZEROFOX INTELLIGENCE

Flash

Threat Collectives Seemingly Announce Collaboration

F-2025-08-13a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Threat Actor, Deep and Dark Web, Ransomware

August 13, 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 August 13, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Threat Collectives Seemingly Announce Collaboration

| Key Findings

- On August 8, 2025, a new account surfaced on instant messaging platform 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, Lap$us, and ShinyHunters.

- In its brief four-day lifespan, posts on the “scattered lapsu$ hunters - The Com HQ SCATTERED SP1D3R HUNTERS” Telegram channel resembled the types of activity Scattered Spider, ShinyHunters, and Lapsu$ are known for within their own Telegram channels.

- In the new Telegram channel, “Shiny”, alleged that BreachForums is now under the control of a French cybercrime law enforcement (LE) unit, with assistance from the U.S. Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI).

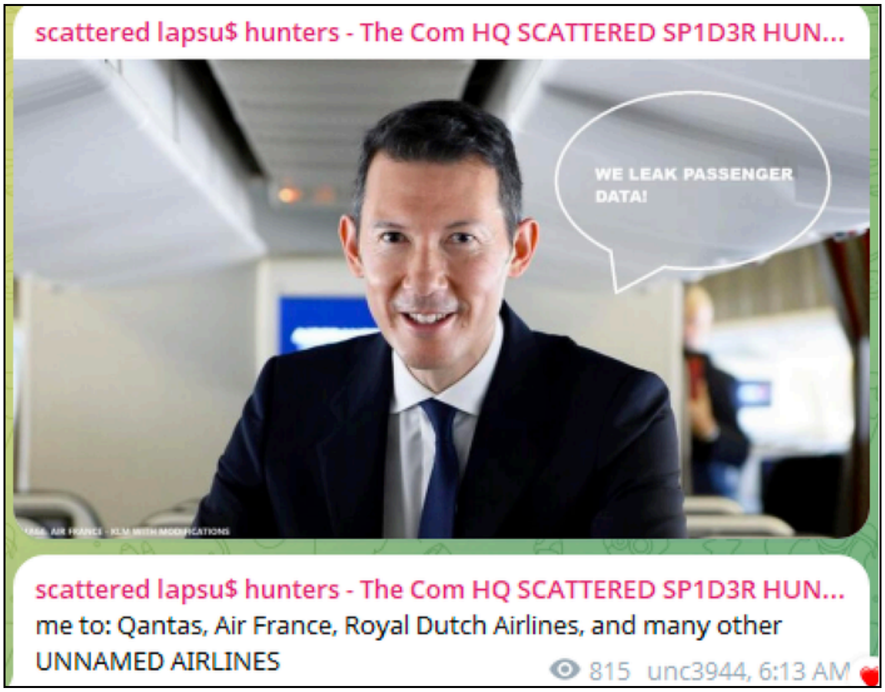
- Although the majority of the claims remain unverified, there is a roughly even chance that the launch of this new Telegram channel signals an intent by Scattered Spider, ShinyHunters, and Lapsu$ to collaborate in future cybercrime operations.

Details

On August 8, 2025, a new Telegram account surfaced named “scattered lapsu$ hunters - The Com HQ SCATTERED SP1D3R HUNTERS”. The channel was launched by individuals that claimed to be part of the prominent Scattered Spider, Lap$us, and ShinyHunters cybercrime collectives. The new Telegram channel posted partially redacted screenshots related to both previously claimed and newly claimed victims.

- The Scattered Spider threat collective has been active since at least 2022 and is likely Western-based and financially motivated. Scattered Spider is known to conduct a variety of malicious activities and has most recently been linked to prominent digital extortion attacks targeting UK-based retail chains Co-op, Harrod’s, and Marks and Spencer.
- Lapsu$ is a threat collective that has been active since at least mid-2021 and has specialized in large-scale social engineering and extortion campaigns. Lapsu$ conducted a number of high-profile attacks throughout 2022, including those targeting Samsung and Nvidia, but its activity has since significantly declined.[1]
- ShinyHunters is a threat collective that emerged in approximately 2022 and is best-known for conducting major data breaches, stealing personally identifiable information (PII) and sensitive corporate information and using it to extort victims and/or selling it on the dark web.
- The new Telegram channel’s launch reflects a long-suspected convergence between Scattered Spider, ShinyHunters, and Lapsu$. Researchers have linked each collective to “The Com”, a loose network of financially motivated actors known for social engineering, data theft, and public extortion.[2]

[1] hXXps://www.techmonitor[.]ai/technology/cybersecurity/lapsus-big-tech-samsung-nvidia
[2] hXXps://www.bankinfosecurity[.]com/scattered-spider-shinyhunters-next-move-leaking-data-a-29170



scattered lapsu$ hunters - The Com HQ SCATTERED SP1D3R HUN...

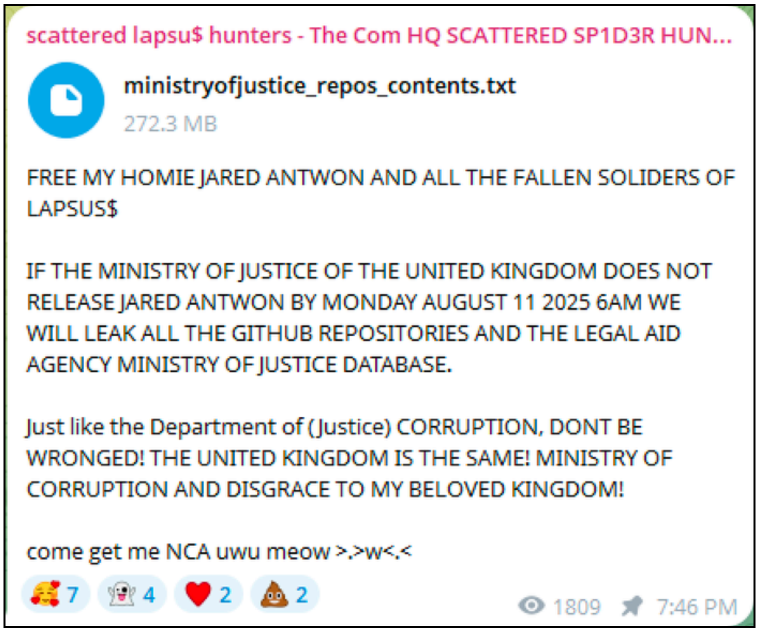
scattered lapsu$ hunters - The Com HQ SCATTERED SP1D3R HUN...
me to: Qantas, Air France, Royal Dutch Airlines, and many other UNNAMED AIRLINES

815 unc3944, 6:13 AM

Post on the new Telegram channel

Source: hXXps://t[.]me/scatteredlapsusp1d3rhunters

On August 11, 2025, 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 Telegram channels operated by Scattered Spider, ShinyHunters, and Lapsu$. Observed posts on the channel included partial data leaks, direct sales pitches, taunts toward security firms, audience polls, and countdown threats targeting high-profile organizations, as well as the promotion of a planned ransomware-as-a-service (RaaS) offering called “SH1NYSP1D3R”. Although the majority of the claims observed on ““scattered lapsu$ hunters - The Com HQ SCATTERED SP1D3R HUNTERS” remain unverified, there is a roughly even chance that the launch of this new Telegram channel signals an intent by Scattered Spider, ShinyHunters, and Lapsu$ to collaborate in future cybercrime operations.



scattered lapsu$ hunters - The Com HQ SCATTERED SP1D3R HUN...

ministryofjustice_repos_contents.txt
272.3 MB

FREE MY HOMIE JARED ANTWON AND ALL THE FALLEN SOLIDERS OF LAPSUS$

IF THE MINISTRY OF JUSTICE OF THE UNITED KINGDOM DOES NOT RELEASE JARED ANTWON BY MONDAY AUGUST 11 2025 6AM WE WILL LEAK ALL THE GITHUB REPOSITORIES AND THE LEGAL AID AGENCY MINISTRY OF JUSTICE DATABASE.

Just like the Department of (Justice) CORRUPTION, DONT BE WRONGED! THE UNITED KINGDOM IS THE SAME! MINISTRY OF CORRUPTION AND DISGRACE TO MY BELOVED KINGDOM!

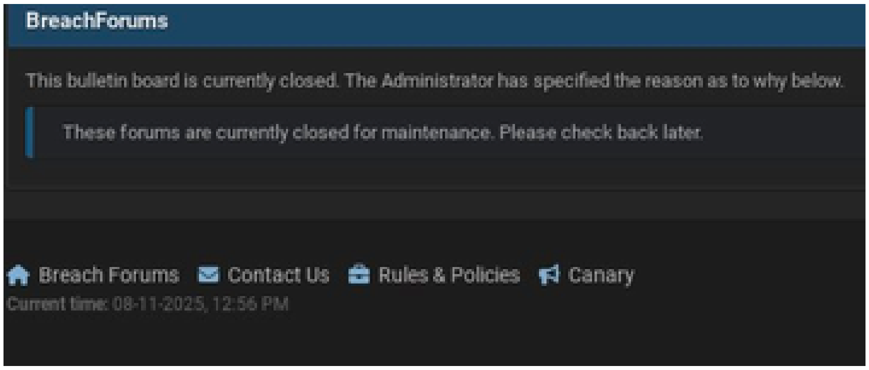
come get me NCA uwu meow >.>w<.<

Scattered lapsu$ hunters' Telegram post

Source: hXXps://t[.]me/scatteredlapsusp1d3rhunters

On August 12, 2025, ZeroFox observed that BreachForums' most recently launched (July 27, 2025) clearnet domain, breachforums[.]hn, and its resurfaced original Tor [.]onion domain were both inaccessible due to 502 gateway errors. In the "scattered lapsu$ hunters - The Com HQ SCATTERED SP1D3R HUNTERS" Telegram channel, Shiny—a well-known administrator of BreachForums and suspected leader of the ShinyHunters threat collective—made several assertions that BreachForums has been compromised. Shiny alleged that the BreachForums site is now under the control of a French cybercrime LE unit, with assistance from the U.S. DOJ and the FBI.

- Shiny asserted on Telegram that all user content on the reinstated forum—including private messages, plaintext passwords, IP addresses, email addresses, and other logged metadata—have been exposed to LE.
- Several BreachForums accounts controlled by Shiny, as well as other administrator accounts, have allegedly been compromised—including "Hollow", "ShinyHunters", and "Anastasia".
- The forum's source code has allegedly been altered to record user activity, which suggests future messages signed with the previous PGP key will likely be untrustworthy.



BreachForums

This bulletin board is currently closed. The Administrator has specified the reason as to why below.

These forums are currently closed for maintenance. Please check back later.

BreachForums bulletin message

Source: ZeroFox Intelligence

In the last week of June 2025, various reports indicated that several key members of BreachForums known by the aliases IntelBroker, ShinyHunters, Hollow, Noct, and Depressed were arrested.[3][4] In the weeks prior to the arrests, ZeroFox concurrently observed both a decline in activity by both IntelBroker and ShinyHunters and several technical issues that disrupted now-defunct iterations of BreachForums, which led to significant speculation about arrests or compromise within DDW forums.

- On June 3, 2025, ShinyHunters made a post alleging that “various agencies” (likely LE entities) had attempted to access BreachForums’ databases amid ongoing disruptions at that time to a prior and now-defunct BreachForums domain (breachforums[.]st).
- Throughout this year alone, BreachForums has experienced several relaunches, new domains, and technical difficulties that are speculated to involve LE interference, although no official explanation has yet been provided.

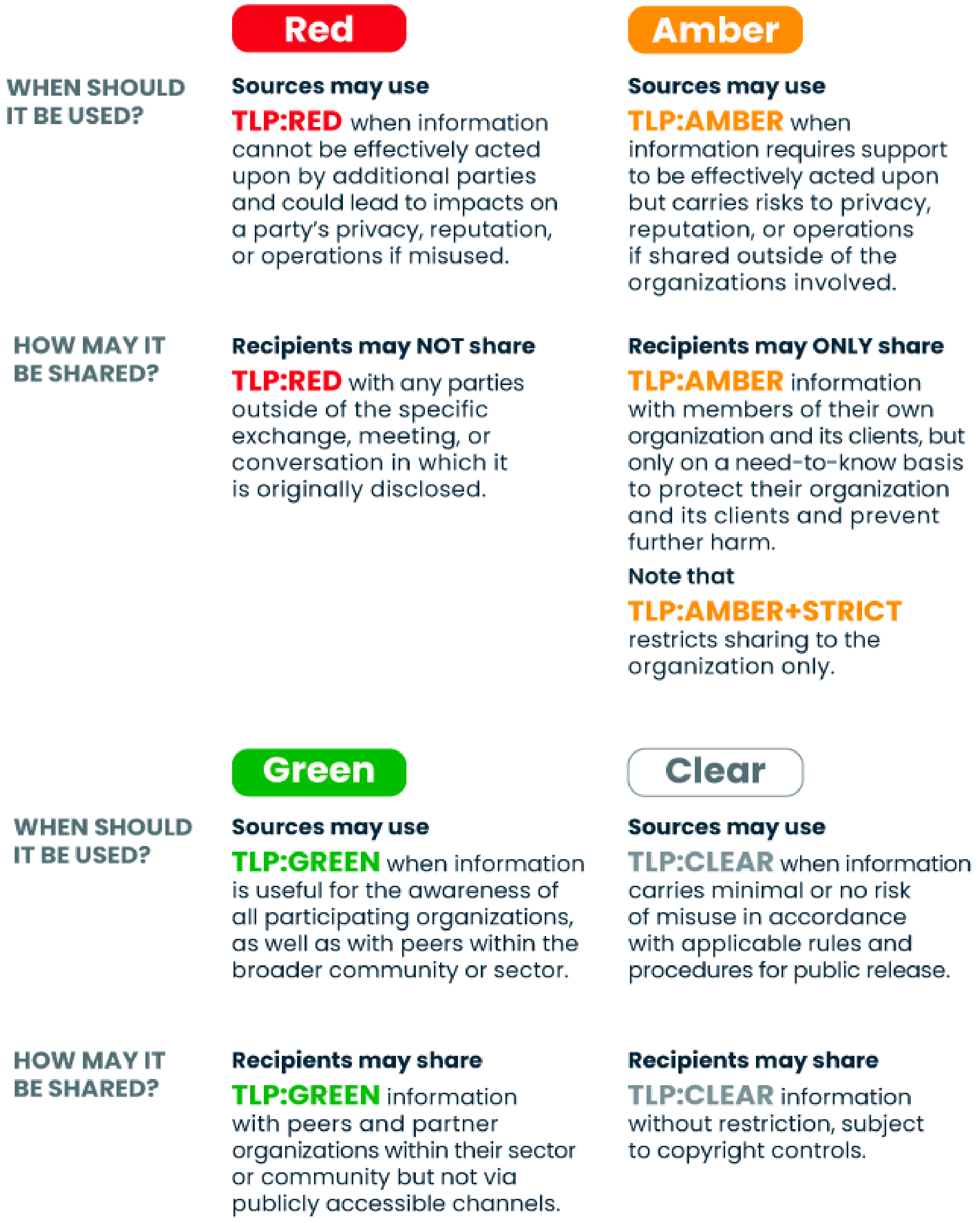
[3] hXXps://www.securityweek[.]com/british-man-suspected-of-being-the-hacker-intelbroker-arrested-charged/

[4] hXXps://siliconangle[.]com/2025/06/25/breachforums-leaders-including-shinyhunters-intelbroker-arrested-france/

Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are updated with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege, and implement network segmentation to separate resources by sensitivity and/or function.
- Implement phishing-resistant multifactor authentication (MFA) and secure and complex password policies, and ensure the use of unique and non-repeated credentials.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud-based servers at least once per year—and ideally more frequently.
- 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 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

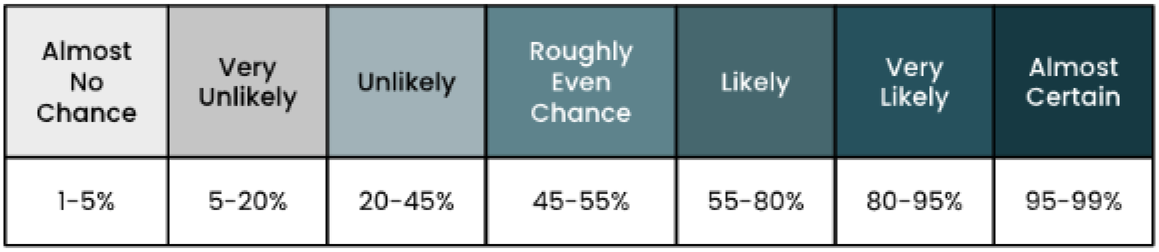


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** **TLP:AMBER** when information requires support to be effectively 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%