ZEROFOX INTELLIGENCE

Flash

DragonForce Announces New Service Updates

F-2025-08-08a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Ransomware, Deep and Dark Web

August 08, 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 07:00 AM (EDT) on August 08, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | DragonForce Announces New Service Updates

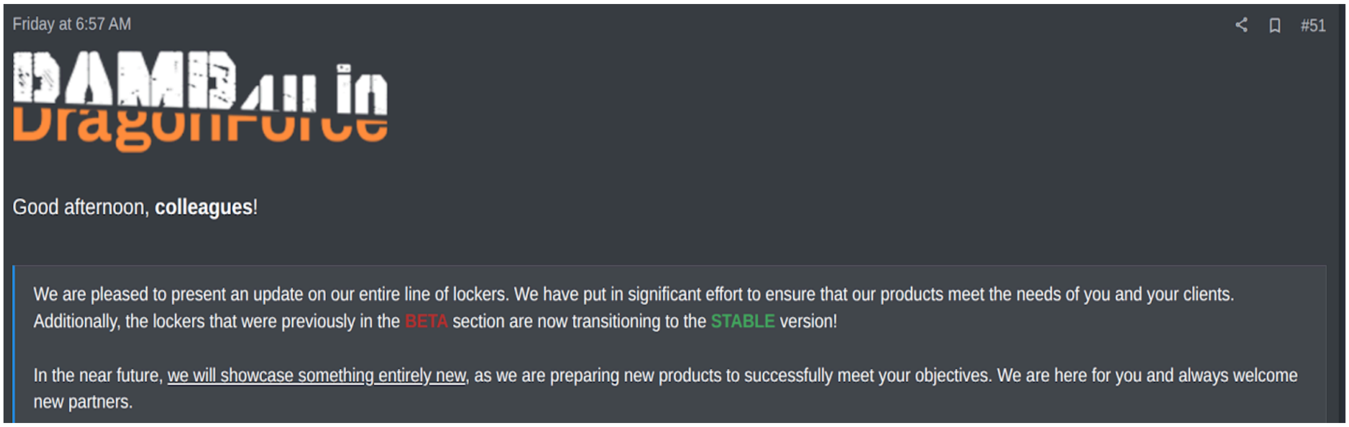
| Key Findings

- On July 31, 2025, an account associated with DragonForce, a ransomware and digital extortion (R&DE) collective, posted on the Russian-speaking dark web forum Russian Anonymous Marketplace (RAMP), announcing various new features for existing services, including updates for its crypto locker.
- In the post on RAMP, the account associated with DragonForce states that the lockers—which refer to the payload that encrypts target files—are now transitioning to a stable version from the previous beta version.
- ZeroFox observed a significant uptick in DragonForce activity, beginning in early April 2025—leading to the collective's most prominent month, in which the group conducted at least 25 separate attacks.
- This latest announcement by DragonForce likely indicates that the collective seeks to remain a prominent threat actor in the R&DE space and attract new affiliates.

Details

On July 31, 2025, an account associated with the R&DE collective DragonForce posted on RAMP, announcing various new features for existing services, including updates for its crypto locker.

- First observed in December 2023, DragonForce has since maintained a relatively low attack tempo compared to other prominent threat collectives, averaging approximately 11 incidents per month.
- At the beginning of Q2 2025, DragonForce raised deep and dark web (DDW) speculation over its alleged relationship with RansomHub, following the latter's cessation of activity in early April 2025 and a series of subsequent DragonForce messages in dark web forums and victim leak pages.
- According to a *BBC* article on May 2, 2025, the media outlet had been in contact with DragonForce ransomware-as-as-service (Raas) operatives, who had claimed responsibility for the targeting of Marks & Spencer (M&S), Co-op, and Harrods.[1] While it remains unverified who was responsible for the attack, the tactics observed closely resemble those of the "Scattered Spider" threat collective.[2]



Good afternoon, **colleagues**!

We are pleased to present an update on our entire line of lockers. We have put in significant effort to ensure that our products meet the needs of you and your clients. Additionally, the lockers that were previously in the BETA section are now transitioning to the STABLE version!

In the near future, we will showcase something entirely new, as we are preparing new products to successfully meet your objectives. We are here for you and always welcome new partners.

DragonForce's RAMP post

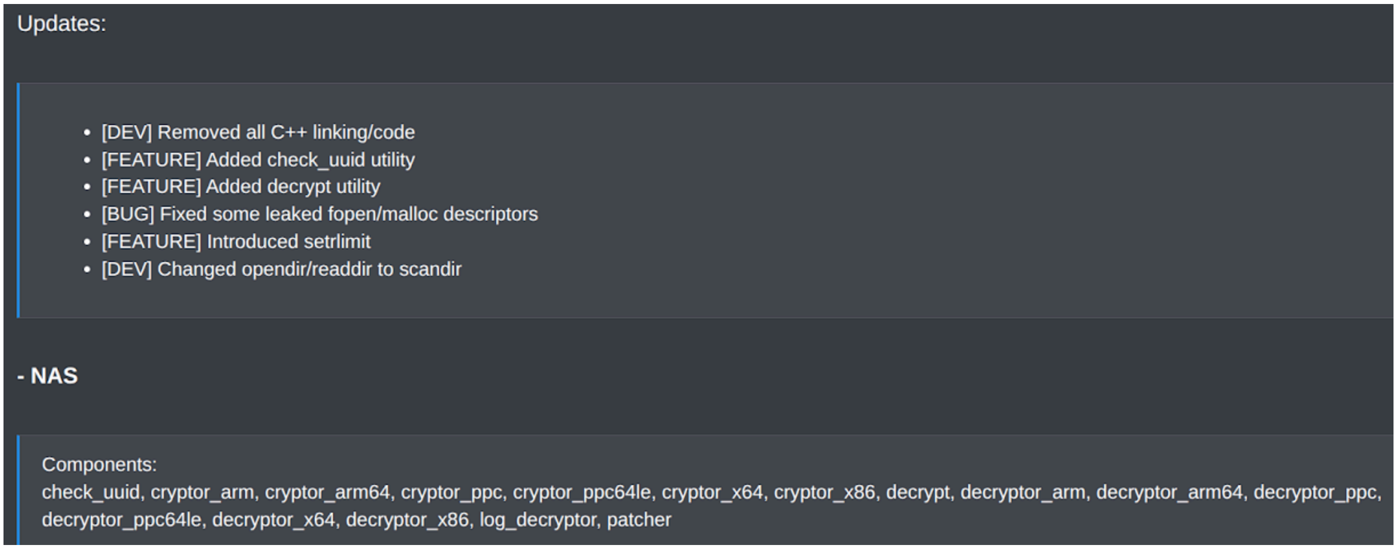
Source: ZeroFox Intelligence

In the post on RAMP, the account associated with DragonForce states that the lockers—which refer to the payload that encrypts target files—are now transitioning to a

[1] hXXps://www.bbc[.]co[.]uk/news/articles/crkx3vy54nzo
[2] *Ibid.*

stable version from the previous beta version. This almost certainly suggests that bugs and malfunctions will be significantly reduced, which will, in turn, very likely increase interest from potential affiliates. Furthermore, the post indicated that the group has removed all C++ programming language, instead opting for Zig.

- Although likely not widely used in malware, Zig is a modern, low-level programming language—meaning the user has more control—that enables faster multi-payload development, lower detection rates, and more stable and efficient code compared to C++.[3] The transition from C++ to Zig represents a tactical evolution in DragonForce's development process and likely also represents efforts to obtain a greater market share in the ransomware space.



Updates:

- [DEV] Removed all C++ linking/code
- [FEATURE] Added check_uuid utility
- [FEATURE] Added decrypt utility
- [BUG] Fixed some leaked fopen/malloc descriptors
- [FEATURE] Introduced setrlimit
- [DEV] Changed opendir/readdir to scandir

- NAS

Components:
check_uuid, cryptor_arm, cryptor_arm64, cryptor_ppc, cryptor_ppc64le, cryptor_x64, cryptor_x86, decrypt, decryptor_arm, decryptor_arm64, decryptor_ppc, decryptor_ppc64le, decryptor_x64, decryptor_x86, log_decryptor, patcher

DragonForce's RAMP post

Source: ZeroFox Intelligence

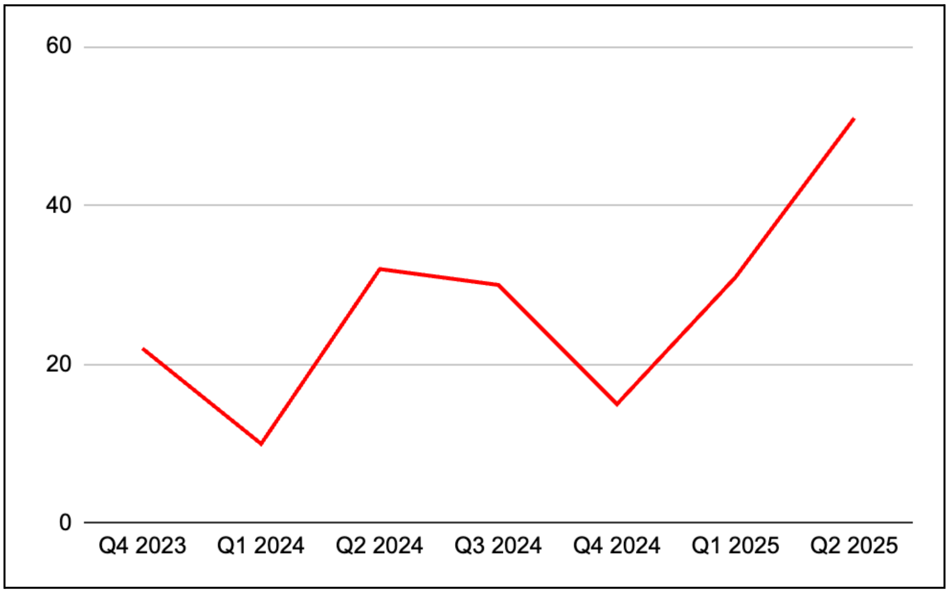
ZeroFox observed a significant uptick in DragonForce activity, beginning in early April 2025—leading to the collective's most prominent month, in which the group conducted at least 25 separate attacks. In Q2 2025, ZeroFox observed at least 51 incidents attributed to DragonForce—a record high for any three-month period for the collective.

- During Q2 2025, the majority of DragonForce attacks (approximately 84 percent) targeted organizations located in the North America region. Notably, this is a significant increase from approximately 38 percent in Q1 2025—which was

[3] hXXps://ziglang[.]org/learn/overview/

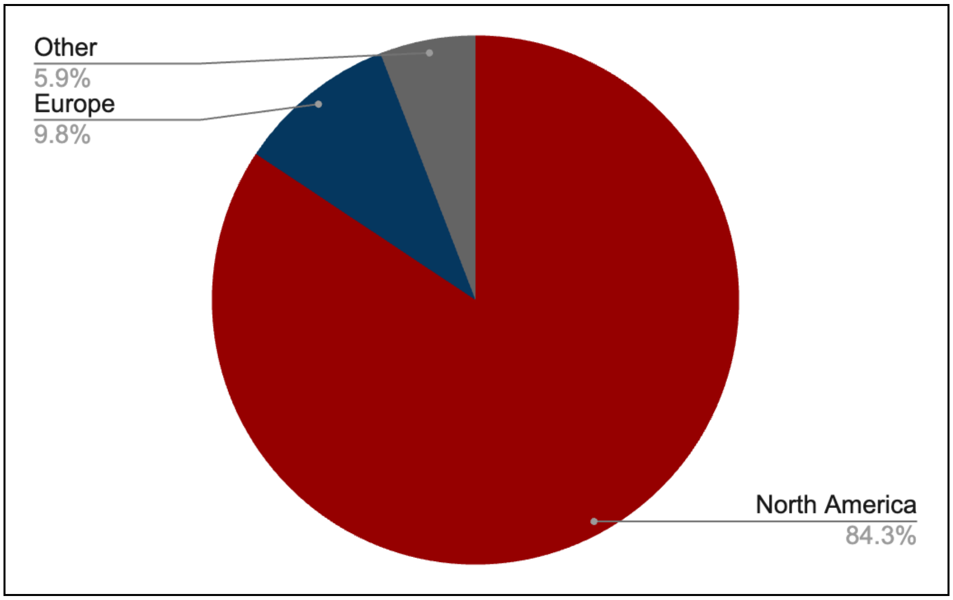
remarkably lower than the 66 percent observed across the R&DE threat landscape.

- Victims located in Europe accounted for approximately 10 percent of DragonForce attacks during Q2 2025, which is lower than the average of approximately 24 percent observed across the R&DE threat landscape.
- During Q2 2025, the majority of DragonForce attacks (approximately 20 percent) targeted organizations within the Professional Services industry. Manufacturing and Legal Services were also heavily targeted and, together with Professional Services, accounted for approximately 48 percent of attacks. These trends are notably different from those observed during Q1 2025, in which the Construction Industry accounted for approximately 29 percent of attacks.



DragonForce attacks by quarter

Source: ZeroFox Intelligence



DragonForce attacks by region in Q2 2025

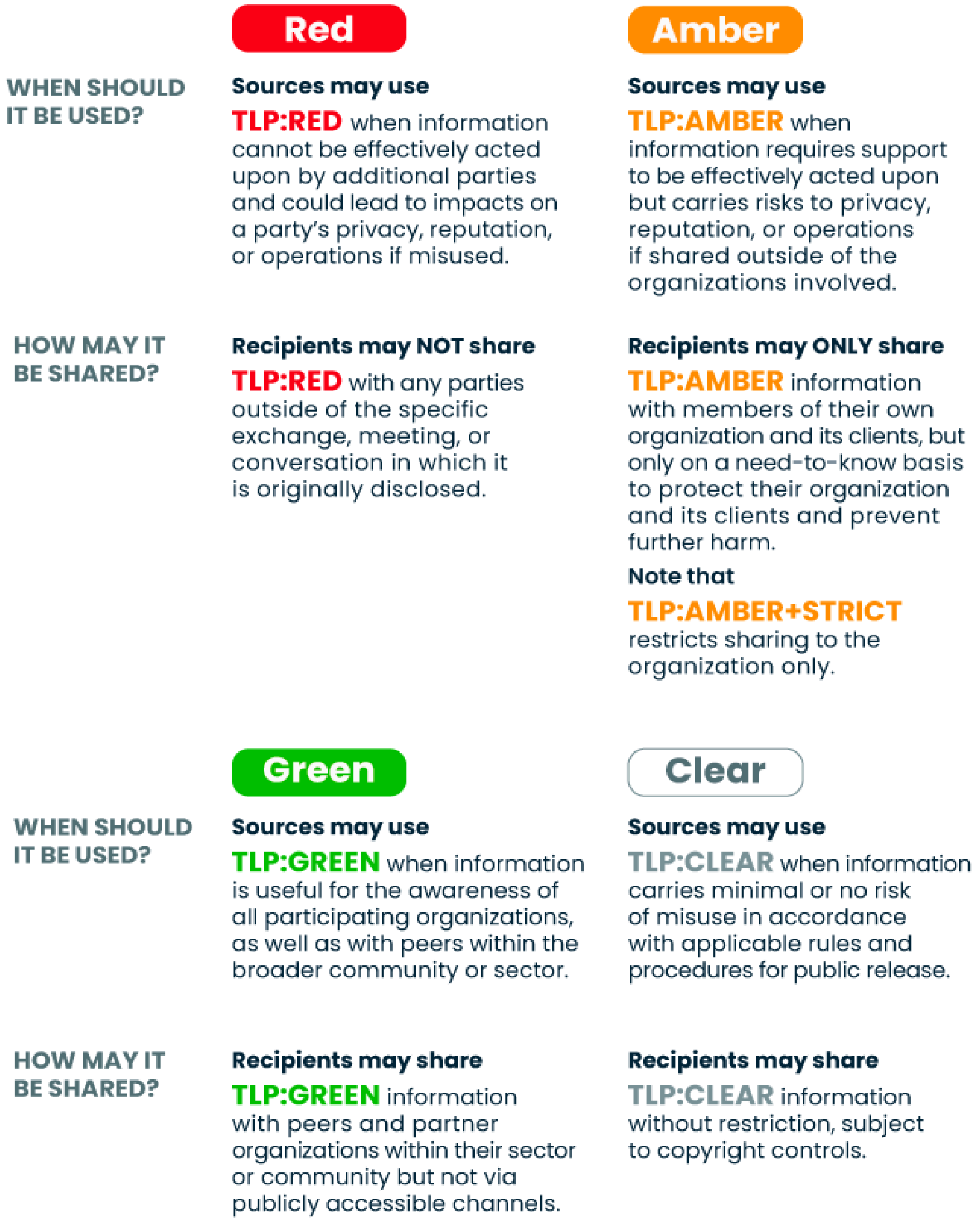
Source: ZeroFox Intelligence

This latest announcement by DragonForce likely indicates that the collective seeks to remain a prominent threat actor in the R&DE space and attract new affiliates. It is likely that DragonForce will continue to disproportionately target North America in Q3 2025 and continue to increase tempo.

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 multi-factor authentication (MFA), secure and complex password policies, and 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

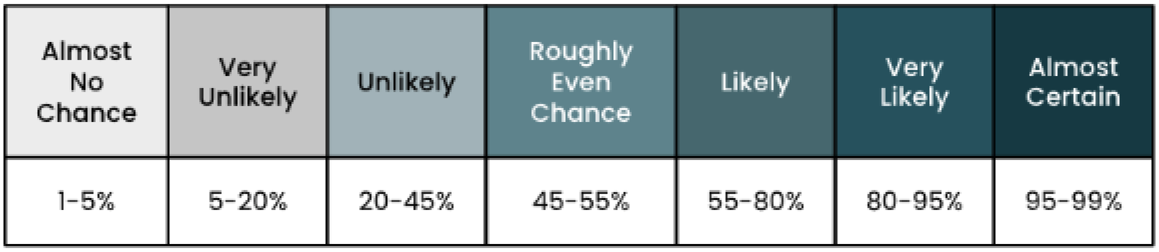


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively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