ZEROFOX INTELLIGENCE

Brief

The Underground Economist: Volume 5, Issue 16

B-2025-08-14b

Classification: TLP:CLEAR

Criticality: LOW

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

August 14, 2025

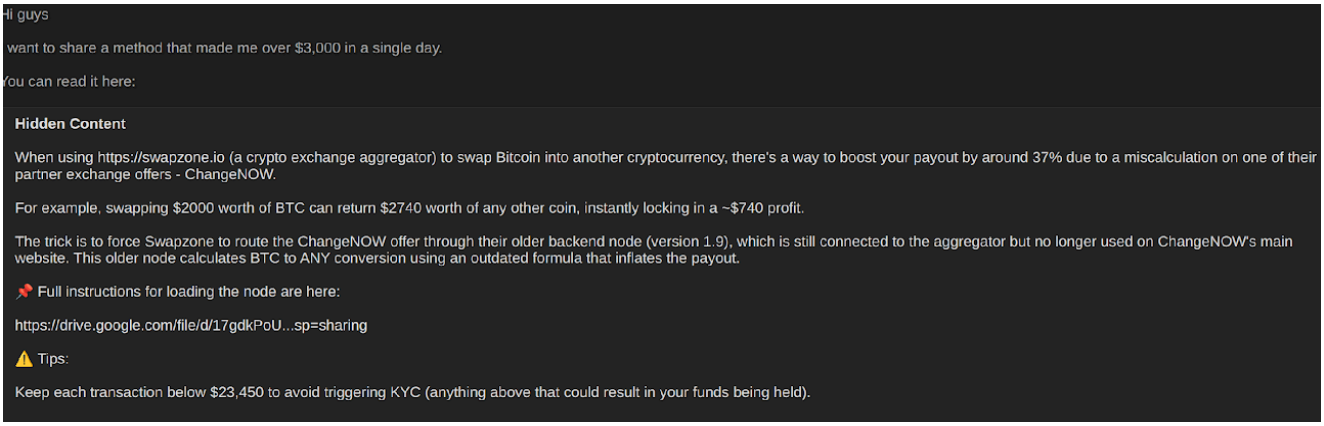
ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot 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 10:30 AM (EDT) on August 14, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Brief | The Underground Economist: Volume 5, Issue 16

| Alleged Cryptocurrency Exchange Glitch Shared on Dark Web Forum

On August 12, 2025, an actor using the alias "Cocaize" posted on the dark web forum DarkForums sharing an allegedly free method to exploit a glitch in the Swapzone cryptocurrency exchange. According to Cocaize, they have made USD 3,000 in a single day using this method.

- Swapzone is an aggregator that connects users to multiple cryptocurrency exchanges through a single interface, allowing them to compare rates and swap cryptocurrencies without needing to deposit funds with Swapzone itself.
- Cocaize joined DarkForums in August 2025 and has so far garnered a negative reputation, which is likely indicative of other users in the forum finding this actor untrustworthy or otherwise illegitimate.



Cocaize's DarkForums post

Source: ZeroFox Intelligence

In the post, Cocaize explained that the advertised technique involves swapping Bitcoin into another cryptocurrency through exchange services on the Swapzone[.]io website. Cocaize stated that a misconfiguration in the Swapzone service enables users to boost payouts by approximately 37 percent due to a miscalculation in one of Swapzone's partner exchange options called ChangeNOW. According to Cocaize, an older backend node of ChangeNOW (version 1.9) allows users to access an old conversion formula that inflates payouts.

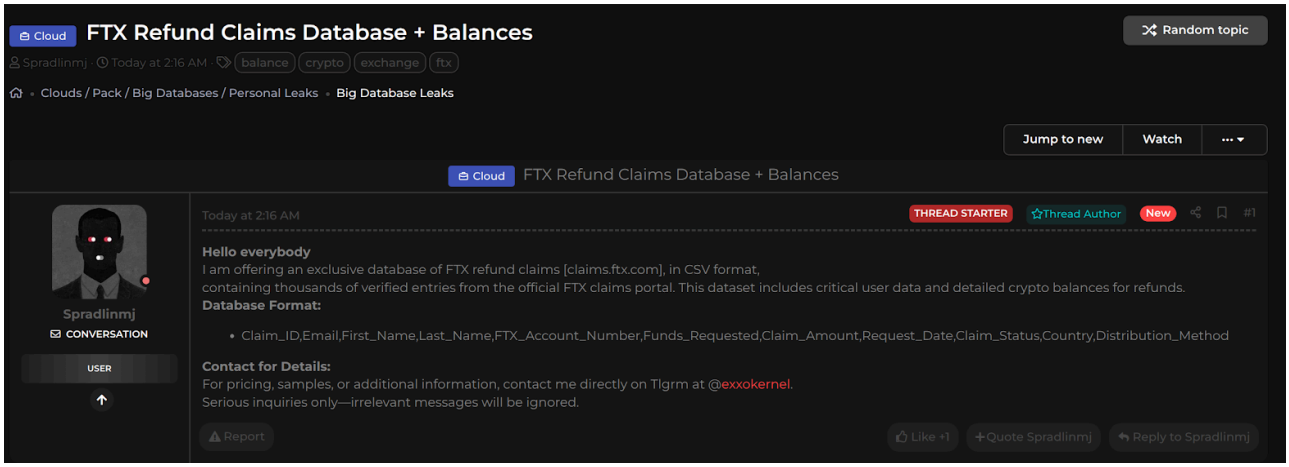
- ChangeNOW is a no-registration cryptocurrency exchange platform that enables crypto-to-crypto and crypto-to-fiat currency swaps and rarely requires Know-Your-Customer (KYC) measures to complete transactions. However, ChangeNOW uses SumSub to assist with KYC measures and compliance and fraud prevention solutions.
- Cocaize stated that keeping transactions below USD 23,450 will avoid triggering KYC procedures.

ZeroFox researchers have not tested the method described by Cocaize due to its illicit nature and cannot verify the authenticity of the claims made by the actor. However, it is likely that several financially motivated actors will be interested in testing the method. If the vulnerability exists, it will likely have a significant impact on cryptocurrency transactions until patched.

Cryptocurrency Exchange FTX Dataset

On August 12, 2025, an actor known as “Spradlinmj” advertised sensitive data from the now-bankrupt cryptocurrency exchange company FTX on the dark web forum LeakBase. The actor claimed to be in possession of an FTX database from the claim.ftx[.]com portal consisting of refund claims, including the balances of affected users.

- The actor indicated prices, samples, and additional information would be privately shared with interested buyers, directing them to message the Telegram account “@exxokernel”.
- Spradlinmj did not disclose any sample data in their post, and the actor currently has no reputation within the forum—making the legitimacy of their claims indeterminable at this time.



Spradlinmj’s LeakBase post

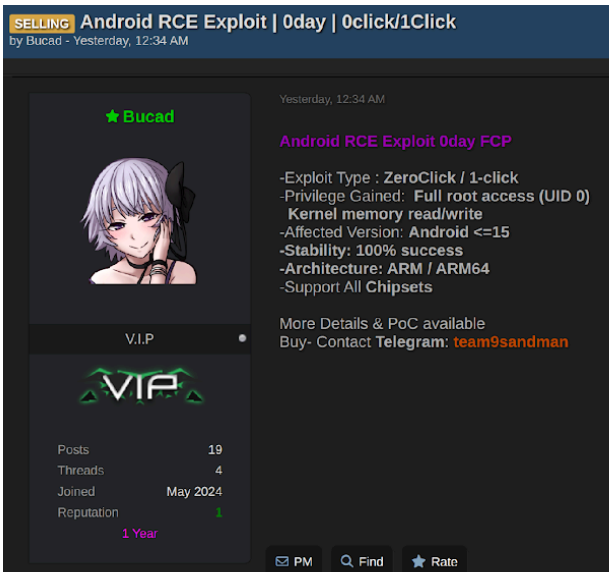
Source: ZeroFox Intelligence

The database fields listed in Spradlinmj’s post include claim ID, email, first name, last name, FTX account number, funds requested, claim amount, request date, claim status, country, and distribution method. The information allegedly included is likely significantly sensitive, as malicious actors could potentially redirect funds intended for legitimate victims of the FTX collapse. This data could also be maliciously leveraged in spear-phishing, impersonation, and social engineering campaigns.

Android Remote Code Execution Zero-day Vulnerability Advertised for Sale on Dark Web Forum

On August 5, 2025, an actor using the alias “Bucad” posted on the dark web forum DarkForums, advertising the sale of an Android remote code execution (RCE) zero-day vulnerability.

- An RCE zero-day vulnerability is a critical, unpatched software flaw that enables an attacker to run their own code on a target system from a distance without needing physical access.
- Bucad joined DarkForums in May 2024 and has since conducted limited activity on the forum; ZeroFox is unable to determine the actor’s credibility at this time.



Bucad’s DarkForums post
Source: ZeroFox Intelligence

Bucad states in the post that the vulnerability is either “ZeroClick” or “1Click”, which indicates the level of user interaction required to trigger it and are common terms used in the context of zero-days. Specifically, the vulnerability allegedly can target Android 15 devices that are running on ARM and ARM64 architectures.

- Android 15 is the latest Android software release and is used on almost all modern Android devices, including phones, tablets, and foldables.

- The price of the vulnerability is not publicly disclosed in the post. According to Bucad, it will only be shared with those that send a private message to the actor via their "team9sandman" Telegram account.

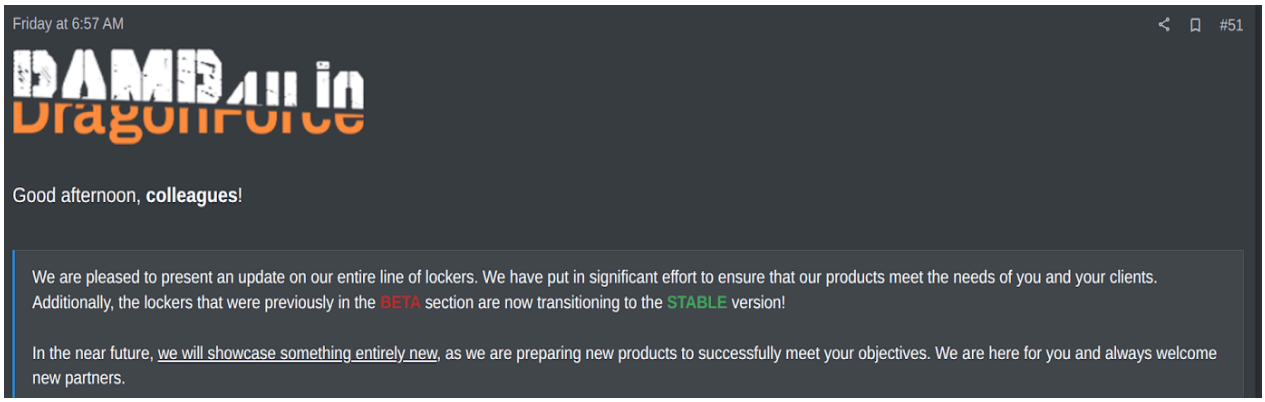
A threat actor could utilize an Android 15 RCE zero-day to essentially take over an Android device, steal sensitive data such as personally identifiable information (PII), and even persist through updates or factory resets. As such, an Android RCE zero-day vulnerability will very likely be sought after by a host of threat actors seeking to conduct an array of malicious activities, including social engineering and extortion.

DragonForce Announces New Service Updates

On July 31, 2025, an account associated with the ransomware and digital extortion (R&DE) collective DragonForce posted in the Russian-language dark web forum RAMP, announcing various new features for existing services—including updates for its crypto locker.

- ZeroFox first observed DragonForce in December 2023. The group 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 garnered 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 published 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 attacks, the tactics observed closely resemble those of the "Scattered Spider" threat collective.[2]

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



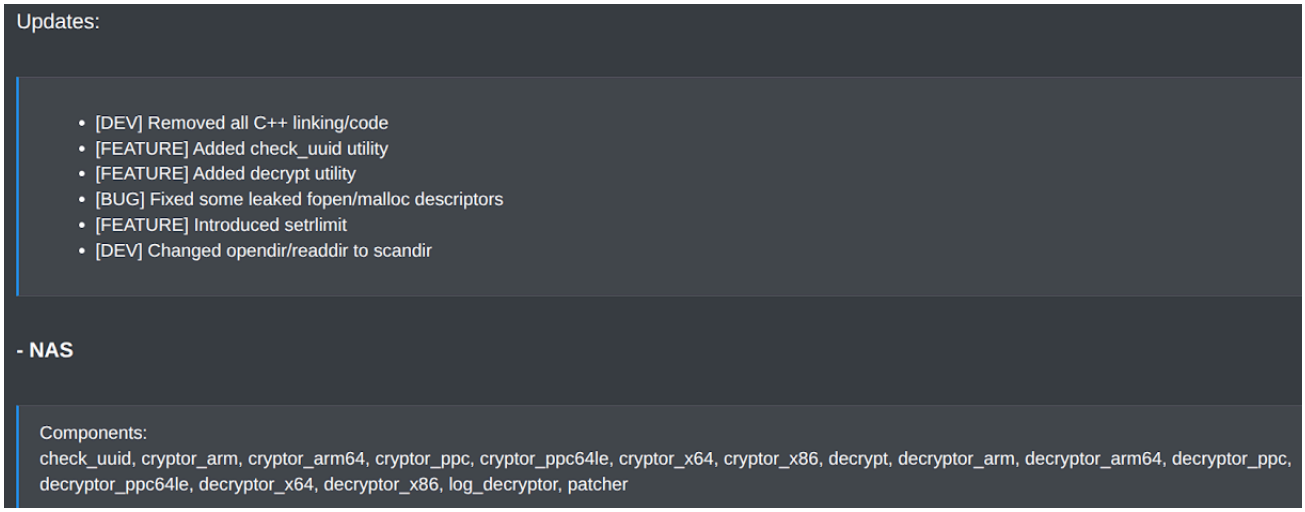
DragonForce's RAMP post

Source: ZeroFox Intelligence

In the post on RAMP, an account associated with DragonForce states that the "lockers" (which refers to the payload that encrypts target files) are now transitioning to a stable version from the previous beta version. This almost certainly suggests that bugs and malfunctions will be significantly reduced, which in turn will 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 likely represents both a tactical evolution in DragonForce's development process and efforts to obtain a greater market share in the ransomware space.

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

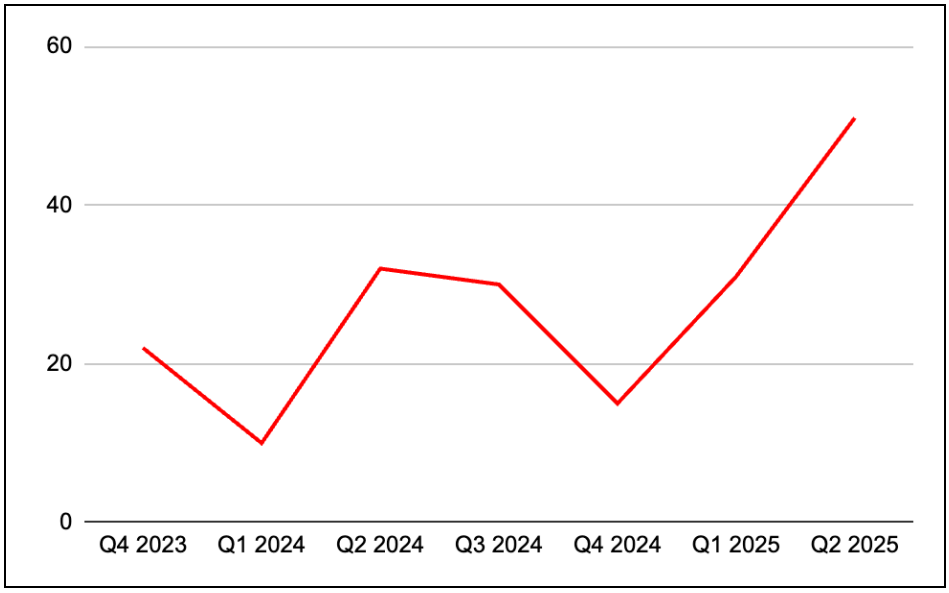


DragonForce's RAMP post

Source: ZeroFox Intelligence

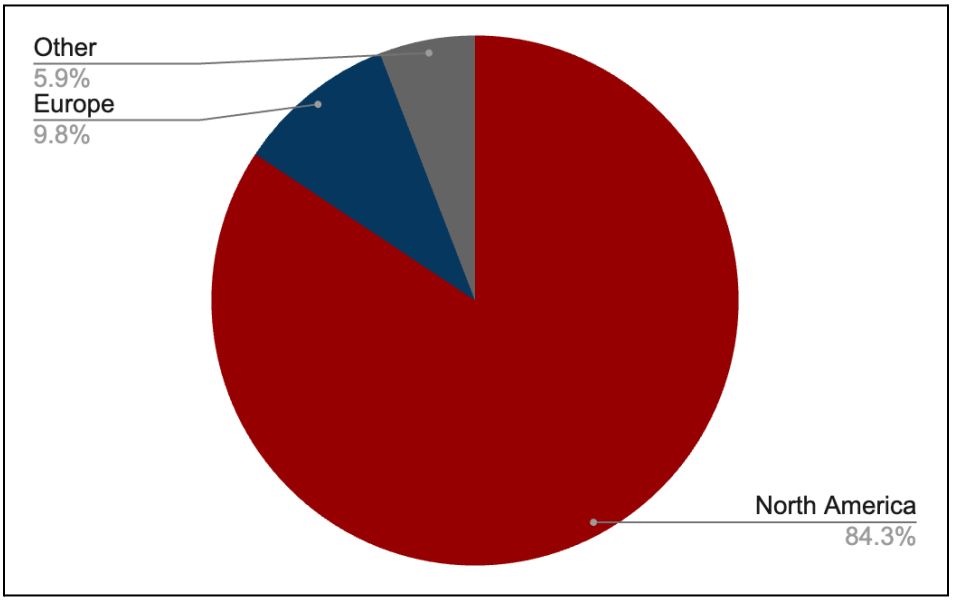
ZeroFox observed a significant uptick in DragonForce activity beginning in early April 2025, leading to the collective's most prominent month (in which the group conducted at least 25 separate attacks). In Q2 2025, ZeroFox observed at least 51 incidents attributed to DragonForce—a record high for any 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 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 both disproportionately target North America in Q3 2025 and increase its attack tempo.

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 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%