ZEROFOX INTELLIGENCE

Brief

The Underground Economist: Volume 5, Issue 20

B-2025-10-09b

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Deep and Dark Web, Threat Actor, Data Breach

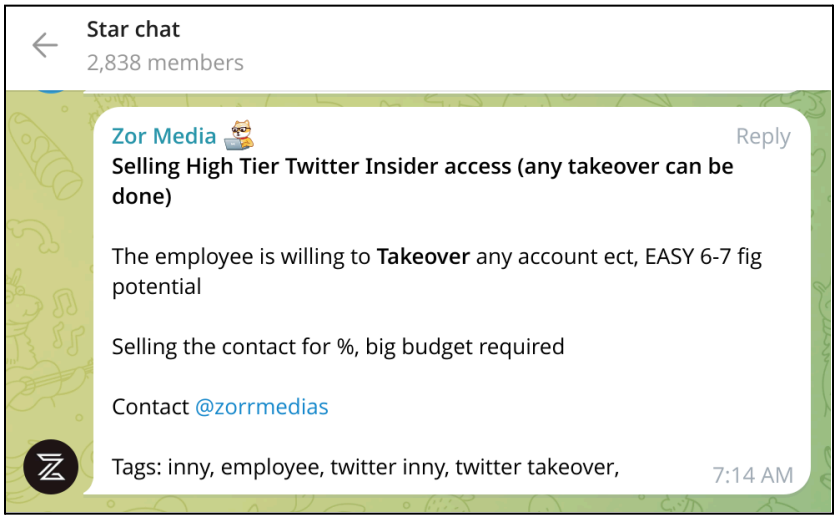
October 09, 2025

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 October 9, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Brief | The Underground Economist: Volume 5, Issue 20

| Threat Actor Alleges Insider Access to X on Telegram

On October 7, 2025, an actor operating under the username "@zorrmedias" posted on the Telegram channel "Star chat", claiming to have high-tier insider access to X (formerly, Twitter). The actor offered to sell contact information for a high-ranking X employee—who is allegedly willing to take over any X account on the social media platform—in return for a percentage of any earnings.



@zorrmedias's Telegram post

Source: ZeroFox Intelligence

The advertisement contains limited information and does not specify a price; however, the actor states that potential buyers require a large budget. Additionally, the post does not specify how the takeovers can return a six to seven figure profit. The lack of details by the untested actor is likely due to the actor attempting to remain overtly cautious and unthwarted by X or more likely because it is a fraudulent offer.

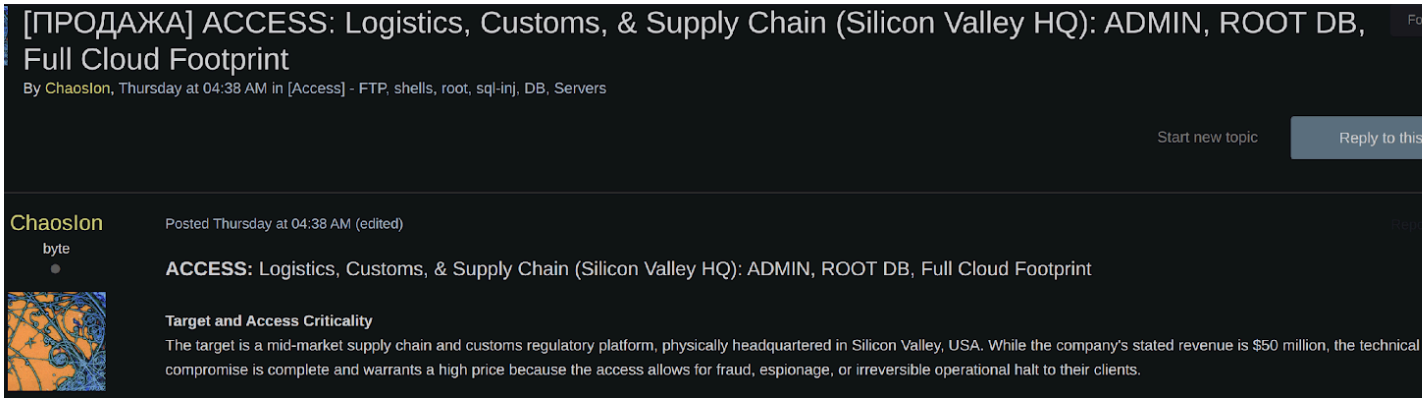
- Compared to deep and dark web (DDW) forum marketplaces (such as Exploit or DarkForums), Telegram is considerably less restrictive and more accessible, without stringent guidelines and reputational scoring processes maintained by well-regarded actors as administrators.
- @zorrmedias is untested, and ZeroFox has not observed significant activity by any actor using the alias in other, more legitimate DDW forums. It is likely that this advertisement is a scam or otherwise fraudulent.
- The Star chat Telegram channel is known for hosting various fraudulent activities, including illicit offers. The content posted to this channel is most likely not credible—largely due to the platform's lack of user verification, easy accessibility to the application, and lack of a reputational earnings process.

However, if this offer is legitimate, such account takeovers could almost certainly cause significant reputational harm to targeted individuals (who are likely those who manage prominent X accounts with large followings). This and other legitimate offers on prominent DDW forums exemplify the increasing trend and risk of insider threat-related incidents to organizations.

Access to Silicon Valley-Based Company Advertised on Dark Web Forum

On October 2, 2025, an actor using the alias “Chaoslon”, posted on the dark web forum Exploit advertising unauthorized access to an unnamed “mid-market supply chain and customs regulatory platform, physically headquartered in Silicon Valley, USA.”

- Chaoslon joined Exploit in August 2025 and has not yet garnered a positive reputation. ZeroFox cannot verify the legitimacy of their claims at this time.



Chaoslon's Exploit post

Source: ZeroFox Intelligence

Chaoslon stated that, while the company's revenue is USD 50 million, the price for the access is BTC 1 (approximately USD 122,000 as of writing), as this reflects fair pricing for the level of technical compromise available. The actor claimed that the technical access on offer comprises the following:

Technical Vector	Compromise Depth	Proof-on-Demand
GitHub Source Code Management (SCM) Admin	Global Org Admin (DevOps Role)	escrow
Production Database	Direct Credentials (Static)	escrow
Amazon Web Services (AWS) Cloud	Global Org Admin (AssumeRole)	escrow

Alleged technical access available

- Administrative control over the company's GitHub SCM would almost certainly grant a potential threat actor full visibility and control over all source code repositories, including the ability to alter, exfiltrate, or inject malicious code into the software supply chain.
- Access to the production database using direct credentials would almost certainly provide a potential threat actor with persistent access to live operational data and personally identifiable information (PII) from the company's customer database.

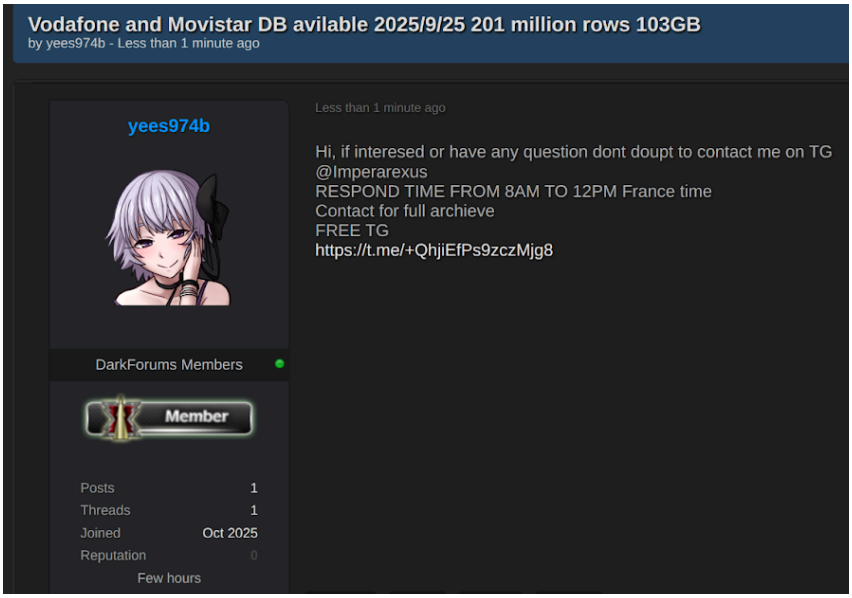
- Access to the company's AWS cloud environment via a Global Organization Admin role would very likely enable full administrative control across AWS services, including storage, networking, and security configuration.
- Chaoslon has indicated that they are willing to provide proof of access via escrow, which adds credibility to their claims.

Together, these claims pose a significant risk of compromise of the company's data and infrastructure layers, which will almost certainly be sought after by various financially motivated actors. The access advertised by Chaoslon would likely be used by potential threat actors to obtain PII for extortion or social engineering campaigns.

Vodafone Customer Database Announced

On October 2, 2025, an untested actor using the alias "yees974b" announced a 103 GB Vodafone and Movistar customer dataset—with allegedly 201 million rows of data—for sale on the dark web forum DarkForums. In the post, the actor claimed that the breach is from September 25, 2025, alleging that the data is not reused or related to previous leaks.

- Vodafone is a U.K.-based multinational telecommunications company that offers mobile, fixed, and Internet of Things (IoT) connectivity, data, and other services globally.
- Movistar is a Spain-based telecommunications provider owned by Telefónica, S.A., a Spain-based multinational telecommunications company.
- Telecommunications data attracts significant interest on DDW forums, as it can be used for SIM swap attacks, account takeovers, and tailored smishing attacks.



yees974b's DarkForums post

Source: ZeroFox Intelligence

Notably, the actor joined DarkForums in October 2025 with only this one post and has not garnered any reputation points thus far; zero reputation points reflects the actor only having made one post, as reputation is garnered through successful and legitimate transactions between sellers and buyers. While reputation does not, especially in this case, solely determine the actor's legitimacy, it indicates the actor's short presence on the forum and potential inexperience or illegitimacy.

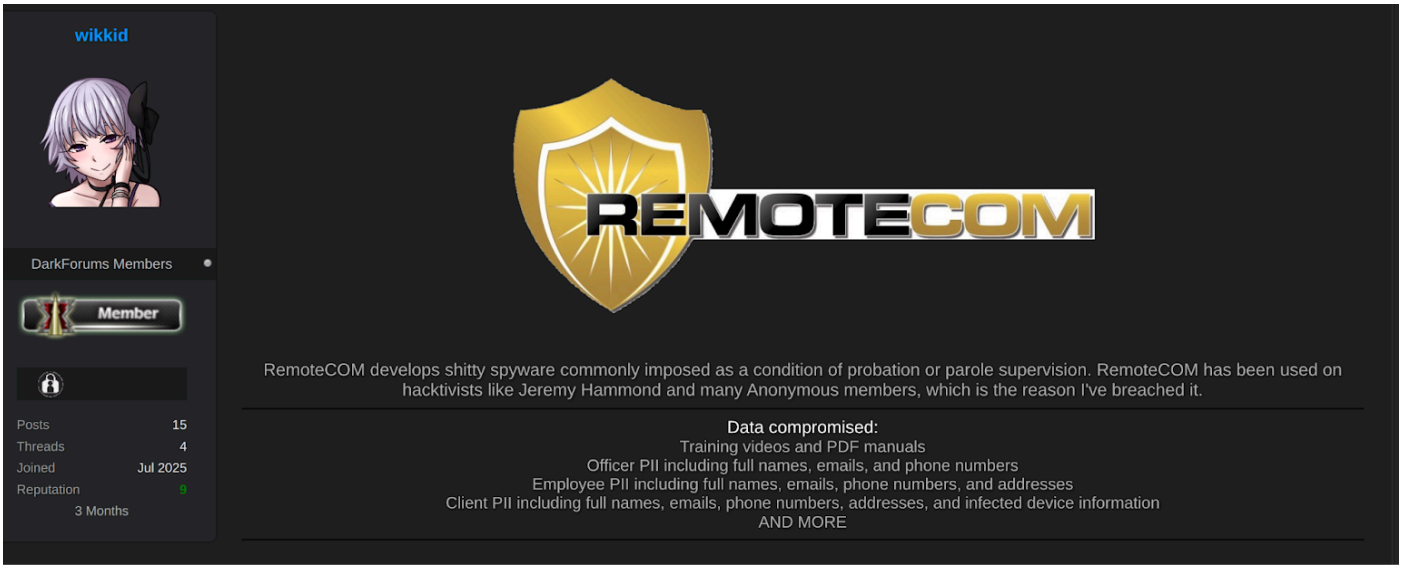
- The actor directed interested buyers to discuss the offer via Telegram; the actor's Telegram handle ("@Imperarexus") and a link to a Telegram channel were also provided.

ZeroFox has observed similar Vodafone-branded advertisements on DDW forums throughout 2025—both legitimate and illegitimate offers likely intended to attract buyers. The prevalence of similar advertisements on DDW forums indicates a likelihood of a spike in SMS phishing attacks pertaining to carrier interactions, plan changes, voicemail resets, as well as fraudulent number-porting and SIM replacement requests.

Monitoring Services Provider's Data Leaked on the DDW

On September 23, 2025, threat actor "wikkid" posted on DarkForums advertising data associated with RemoteCOM, a U.S.-based monitoring service company. The actor claimed to have successfully breached RemoteCOM and obtained PII of approximately 14,000 monitored individuals and 6,900 law enforcement contacts.

- The actor shared the RemoteCOM leak as a seemingly free service, stating that RemoteCOM has been used on hacktivists such as Jeremy Hammond and members of the Anonymous group, which is why they breached the company's data. Comments under the post thanked the actor, and one called the data "promising."
- A member of DarkForums since July 2025 with a moderately positive reputation, wikkid has a track record of posting other data leaks on DarkForums, with some drawing more than 15,000 replies and largely positive reactions, indicating the actor is likely credible.



wikkid's DarkForums post

Source: ZeroFox Intelligence

The actor provided a list of allegedly compromised PII related to law enforcement officers, employees, and clients, which includes full names, emails, phone numbers, addresses, infected device information, and "MORE" (no further details were provided).

- The leaked information is likely to be used by potential threat actors for various purposes, including impersonating officers or extracting additional personal data for social engineering campaigns.

ZeroFox assesses the leak to be likely genuine, given the actor's credible reputation and history, absence of a financial motive, and the high sensitivity of some of the leaked data. The leak will likely garner the attention of various threat actors, who could use the surveillance data to conduct several damaging cyberattacks against the compromised victims.

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%