ZEROFOX INTELLIGENCE

Brief

The Underground Economist: Volume 6, Issue 6

B-2026-03-13a

Classification: TLP:CLEAR

Criticality: LOW

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

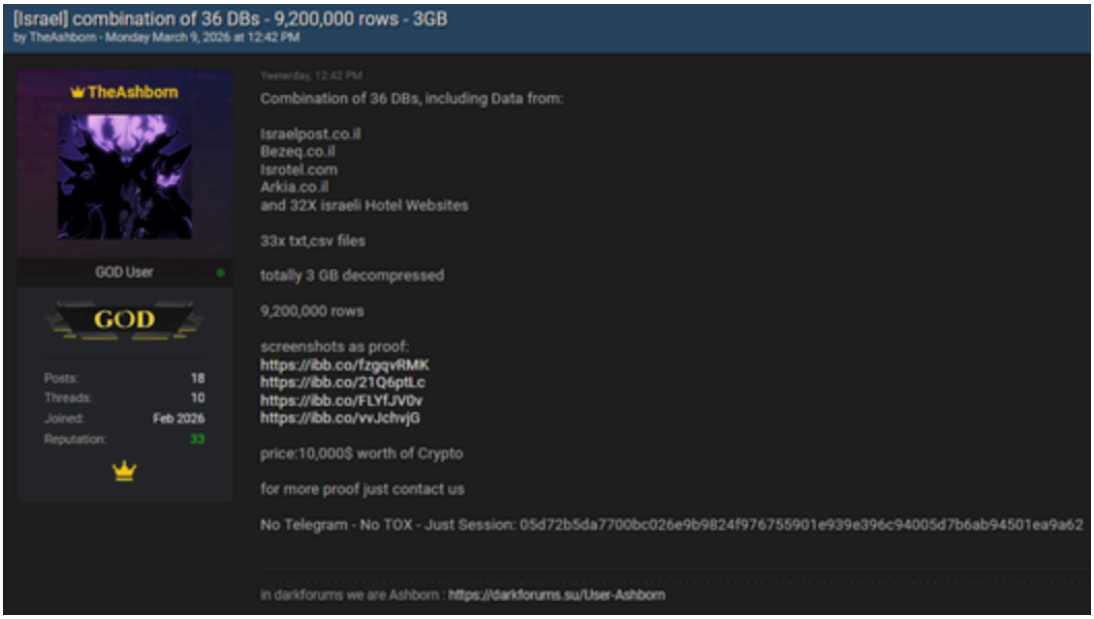
March 13, 2026

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 March 12, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Brief | The Underground Economist: Volume 6, Issue 6

| Personal Data Related to Middle-East Entities

Over the period of March 9–10, 2026, newly-registered and untested threat actor "TheAshborn" made a series of posts on the dark web forum BreachForums advertising the sale of databases pertaining to multiple Middle Eastern companies and government entities.



TheAshborn's first BreachForums post
Source: ZeroFox Intelligence

TheAshborn claimed to be in possession of the following data sets:

- **Israel-based**: The threat actor claims to possess 36 unique databases from several Israeli entities, including the Israel Postal Company, Bezeq, Isrotel Hotels, Arkia, and 32 other hotel websites. The combined dataset allegedly contains 9.2 million rows of data, with an asking price of USD 10,000 worth of crypto.
- **Lekhwiya Dataset (Qatar)**: This dataset is allegedly associated with Lekhwiya, a Qatar-based Internal Security Force agency, and contains the sensitive personally identifiable information (PII) of more than 1,900 agency personnel. The asking price is currently set at USD 10,000.
- **Jazeera Airways Dataset (Kuwait)**: This dataset allegedly belongs to Kuwait-based Jazeera Airways and contains 15 million rows of data, including full names and email addresses. The currently available data spans from 2020 to 2023; the actor explicitly noted that more recent data (2023–2026) is not for sale at this time.
- **Iranian Nationals in the UAE Dataset**: This dataset claims to contain information on Iranian nationals residing in the United Arab Emirates (UAE). It allegedly includes 180,000 records featuring names, physical addresses, email addresses, and dates of birth.

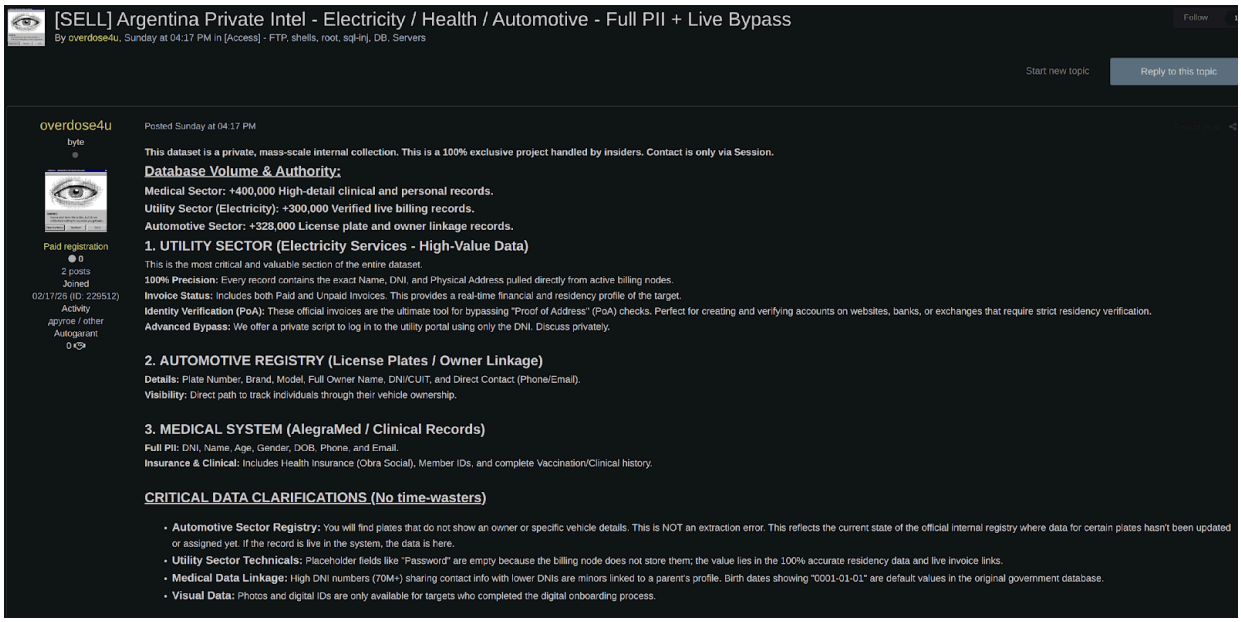
ZeroFox observed that the posts published by TheAshborn contain alleged access and data previously advertised by a high-frequency threat actor operating under the alias "BIG-BROTHER". While the sample URL provided by TheAshborn matches one previously used by BIG-BROTHER, the session ID is different. It is unclear why a new moniker is being used, given BIG-BROTHER's established presence on other forums; however there is a roughly even chance that TheAshborn is a new alias being used by BIG-BROTHER.

In light of the ongoing conflict in the Middle East, it is likely that data sets such as the ones listed above are of high interest to a variety of politically motivated threat actors seeking to inflict harm on their intended target. Notably, the datasets advertised include victims on both sides of the conflict, indicating that TheAshborn is almost certainly politically agnostic and solely financially motivated.

Alleged Argentinian Data Sets Advertised on Exploit

On March 8, 2026, newly registered and untested threat actor "overdose4u" advertised unspecified critical data related to Argentina for sale on the dark web forum Exploit. According to the seller, they are offer exclusive and private intelligence allegedly provided by insiders that has been exfiltrated via a large-scale operation. The actor claims this collection includes data from three different categories:

- Medical Sector: More than 400,000 highly-detailed clinical and personal records
- Utility Sector (Electricity): 300,000 verified live billing records
- Automotive Sector: More than 328,000 license plate and owner linkage records



overdose4u's Exploit post
Source: ZeroFox Intelligence

The most crucial data allegedly provided by the actor is very likely the medical data. Based on details given by the seller, this collection contains:

- Full PII
- DNI (national identity cards)
- Age

- Name
- Gender
- DOB (date of birth)
- Phone number
- Email address
- Insurance and Clinical Information that includes Health Insurance (Obra Social), Member IDs, and Complete Vaccination/Clinical History

The second most critical data supposedly offered by overdose4u is likely the utility sector information, which pertains to electricity services. The actor states that this is the most critical and valuable section of the entire dataset. Based on the seller's information, each of these records comes with valid:

- Names
- DNI
- Physical addresses pulled directly from active billing notes
- Invoice status that includes both paid and unpaid invoices, which provides the buyer with a real-time financial residency profile of the targeted person
- Identity verification data that can be used to bypass "Proof of Address" (PoA) for almost anything issued digitally

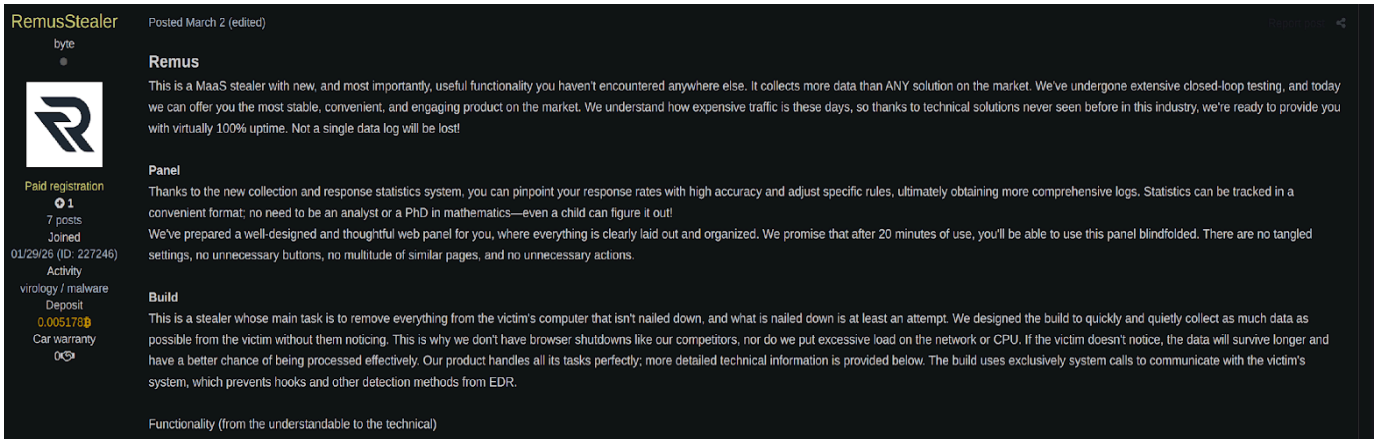
The listed price is USD 2,000 for 1,000 full records from each category or USD 500,000 for the exclusive sale of the full data set, , which overdose4u indicates is negotiable in private. ZeroFox is unable to determine the legitimacy of the actor or their claims; however, overdose4u has a limited presence on the forum with few posts and interactions, decreasing the likelihood that their claims are credible.

If the actor's information is confirmed as authentic, the alleged data would very likely impact most sectors in Argentina. There is likely an unlimited number of ways that such information could be exploited or monetized by malicious actors, but ZeroFox assesses that banks and crypto exchanges will likely suffer the biggest impact from thousands of fake account applications, which could be used for money-laundering and all other types of financial fraud.

New InfoStealer Announced by Threat Actor

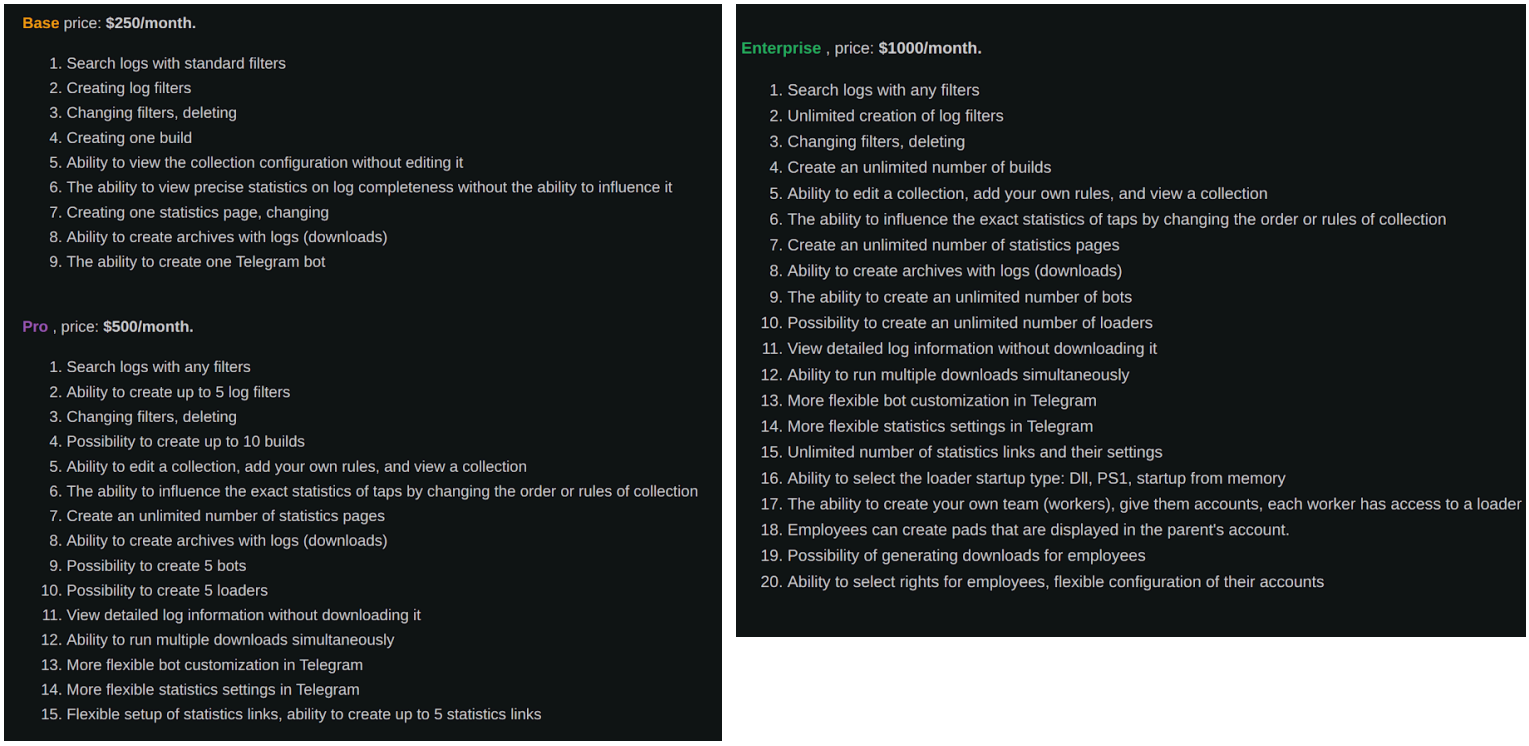
On March 2, 2026, newly registered and untested threat actor "RemusStealer" announced a new malware-as-a-service (MaaS) infostealer called "Remus" on the dark web forum Exploit. RemusStealer stated anyone could lease the service and there were three pricing options which range from USD 250–USD 1,000 per month.

- Although new to Exploit, RemusStealer provided some positive feedback they had received from affiliates, which demonstrates an increased level of credibility and was almost certainly intended to boost interest and potential sales.
- The listed prices were USD 250 per month for the basic version, USD 500 per month for the pro version, and USD 1,000 per month for the enterprise version. Each Remus option has additional functionalities to reflect the increased cost.



RemusStealer's Exploit post
Source: ZeroFox Intelligence

In the post, RemusStealer described the stealer panel as one of the most user-friendly available to potential affiliates. Notably, in contrast to other stealers that require users to have advanced technical skills, Remus appears to be designed to aid lower skilled fraudsters with malware campaigns.



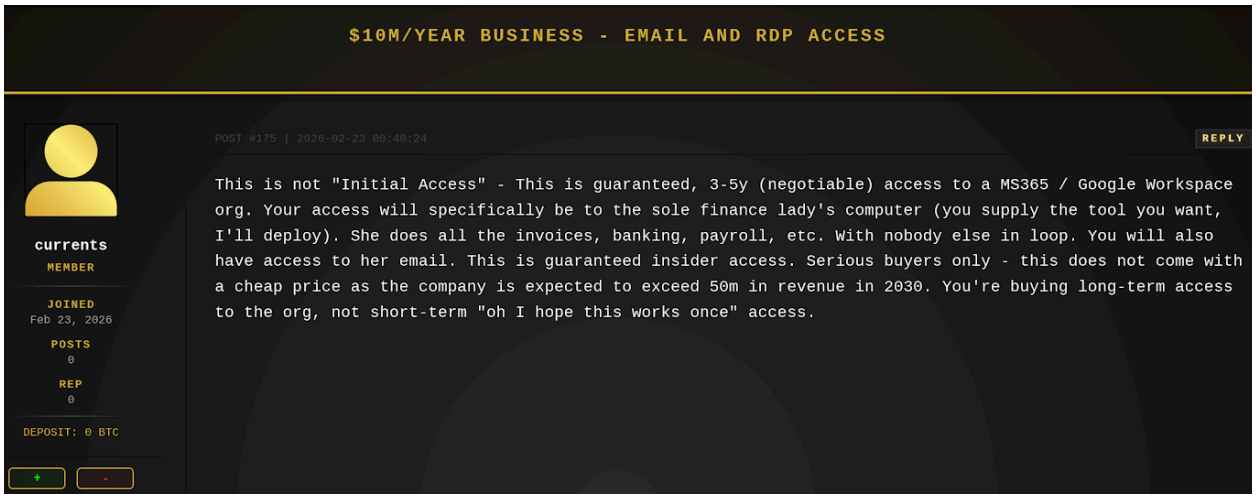
Remus' list of functionalities
Source: ZeroFox Intelligence

The various pricing options, feedback, and significant ease of access and user interface will almost certainly elicit significant interest from a host of threat actors. Infostealers are constantly evolving and developing to match advancements in technology and affiliate needs. It is very likely that RemusStealer's offering will gain traction in the infostealer marketplace, especially amongst users with low technical skill, which will prompt response from other infostealer services to match the user operability offered by Remus.

Long-Term Insider Access Advertised for Sale

On February 23, 2026, newly registered and untested threat actor "currents" advertised the sale of insider access to an unnamed organization on the private dark web forum ZeroDay. According to the actor, the offer includes guaranteed access to the target organization's Microsoft 365/Google Workspace business for three to five years; the post did not include pricing for this long-term access.

- ZeroDay is a new dark web forum launched in February 2026. As such, no threat actors on the forum have gained any positive reputation yet, and ZeroFox cannot determine the credibility of forum postings at this time.
- Guaranteeing access lasting three to five years is highly uncommon on the deep and dark web (DDW) and almost certainly represents a long-term operational campaign.



currents' ZeroDay post
Source: ZeroFox Intelligence

According to the post, the access would be provided through the computer of an unknown female employee whose responsibilities at the company are financial in nature. The employee allegedly handles all invoices, banking operations, and payroll.

- The victim company is allegedly expected to exceed USD 50 million in revenue by 2030, which will almost certainly justify the significant price for access.
- It is common practice amongst threat actors to provide sparse details about the target company in order to avoid detection and prevent victim identification.

It is unlikely like the intent behind such access is ransomware deployment; rather, it is more likely to be manipulation, corporate espionage, and access to valuable information from a company that is allegedly still in development.

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%

Untested	Moderately Credible	Well-regarded	Prominent
Has garnered no reputation, credibility can not be determined.	Has made up to 10 transactions, has been active on forum for at least 3 months.	Has at least 10 transactions, has been active on forum for 3 months to 1 year.	One of the most well-known and credible threat actors on the site. Long-term established presence on the forum, more than 1 year.

Chart Title