ZEROFOX INTELLIGENCE

Brief

The Underground Economist: Volume 6, Issue 8

B-2026-04-09b

Classification: TLP:CLEAR

Criticality: LOW

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

April 9, 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 April 9, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Brief | The Underground Economist: Volume 6, Issue 8

| Alleged Network Access to a U.S.-based "Top 10" Global Aerospace and Defense Corporation

On April 8, 2026, well-regarded threat actor "miyako" advertised allegedly unauthorized network access on the deep and dark web (DDW) forum PwnForums to an unnamed U.S.-based global aerospace and defense corporation that supposedly has a revenue of USD 20 billion. The seller's asking price is USD 1,000 for access to the corporation's firewall device on a Linux workstation, with permissions including root remote command execution (RCE) and shell access.

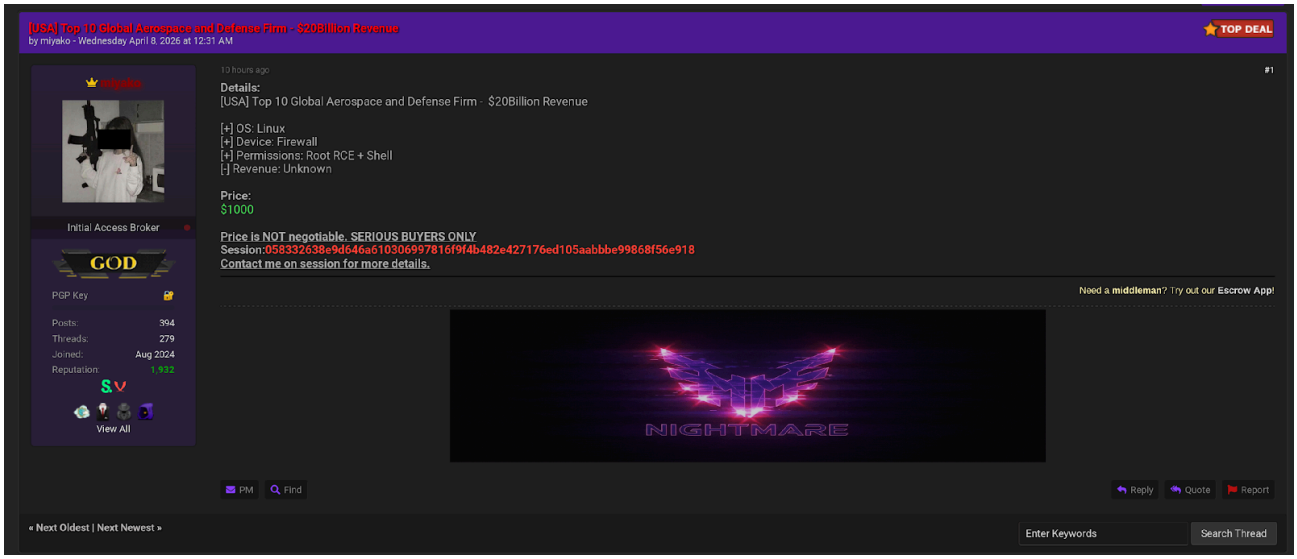
- Based on the actor's description, the targeted company is likely U.S.-based L3Harris Technologies, as this company reports between USD 19 billion and USD 21 billion in revenue.
- L3Harris Technologies is a major U.S. government contractor, ranking in the top 10 of all defense companies based on revenue from government contracts.[1] This position in the industry makes it very likely that the company has access to data that would make the offer of initial access valuable to potential buyers.

Miyako is well-known for selling initial network access to large companies at relatively low prices. The actor likely sets considerably lower prices due to their claimed access

[1] hXXps://people.defensenews[.]com/top-100/

either being not well-established or only capable of leading to non-sensitive segments of the victim's network.

- However, skilled cyberattackers could still very likely exploit even limited access to escalate their presence in the victim's environment.



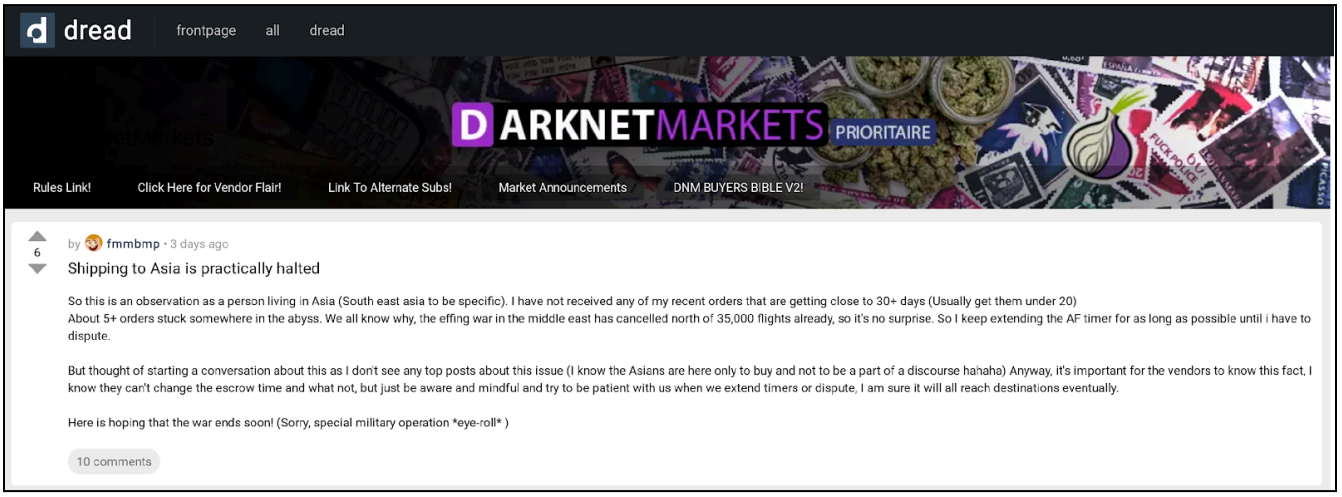
Miyako's post on PwnForums

Source: ZeroFox Intelligence

If confirmed, this would almost certainly be valuable to cybercriminals, as it would very likely provide access to confidential data—including employee personal information—and likely reveal sensitive U.S. government data. Miyako is likely offering legitimate access to L3Harris Technologies, but given the actor's history, the access is very likely limited and would require a skilled cybercriminal to exploit it.

Dark Web Drug Shipments to Asia Affected by Middle East Conflict

On April 5, 2026, moderately credible user "fmmbmp" posted an observation on the dark web forum Dread that drug shipments from darknet markets to Asia have almost completely halted.



fmmbmp's post on Dread

Source: ZeroFox Intelligence

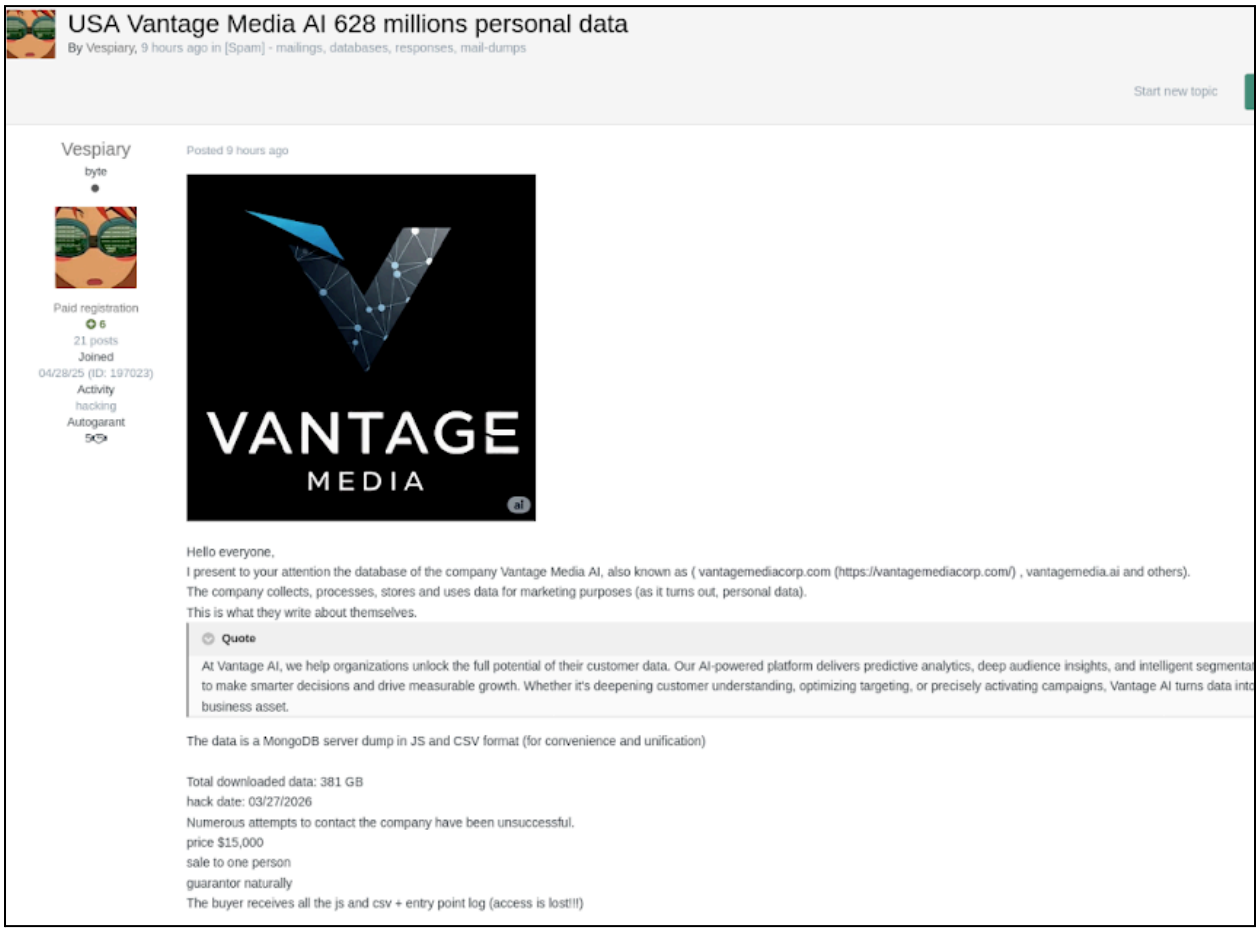
Based on the actor's observations, deliveries would typically take approximately 20 days to arrive; however, they stated that they had not received any of their recent orders, which had been placed more than 30 days ago. The actor attributed the disruption to the ongoing conflict in the Middle East and further explained that, due to the cancellation of more than 35,000 flights in the region, such delays are not surprising.

It is almost certain that the dark web drug trade is experiencing significant delays and disruptions due to supply chain issues caused by the ongoing conflict in the Middle East. There is a roughly even chance that, as the conflict extends, dark web drug trade will experience further volatility. Due to flight cancellations, it is likely that drug suppliers are seeking alternative options, such as sea freight or land routes.

628 Million Records from Vantage Media AI Advertised on the Dark Web

On April 1, 2026, moderately credible threat actor "Vespiary" advertised a 381 GB data set associated with the U.S.-based Vantage Media AI on the predominantly Russian-language dark web forum Exploit. The data set, priced at USD 15,000, allegedly comprises 628 million records of personally identifiable information (PII), including email addresses, phone numbers, physical addresses, full names, employment details, IP addresses, genders, political affiliations, religions, dates of birth, and LinkedIn profile URLs.

- The actor stated that the data set will be sold to a single buyer, likely suggesting a controlled or exclusive sale model.
- Vantage Media AI is a U.S.-based consumer data and marketing intelligence platform that helps businesses optimize their digital strategies through predictive analytics and enriched audience insights.



Vespiary's post on Exploit

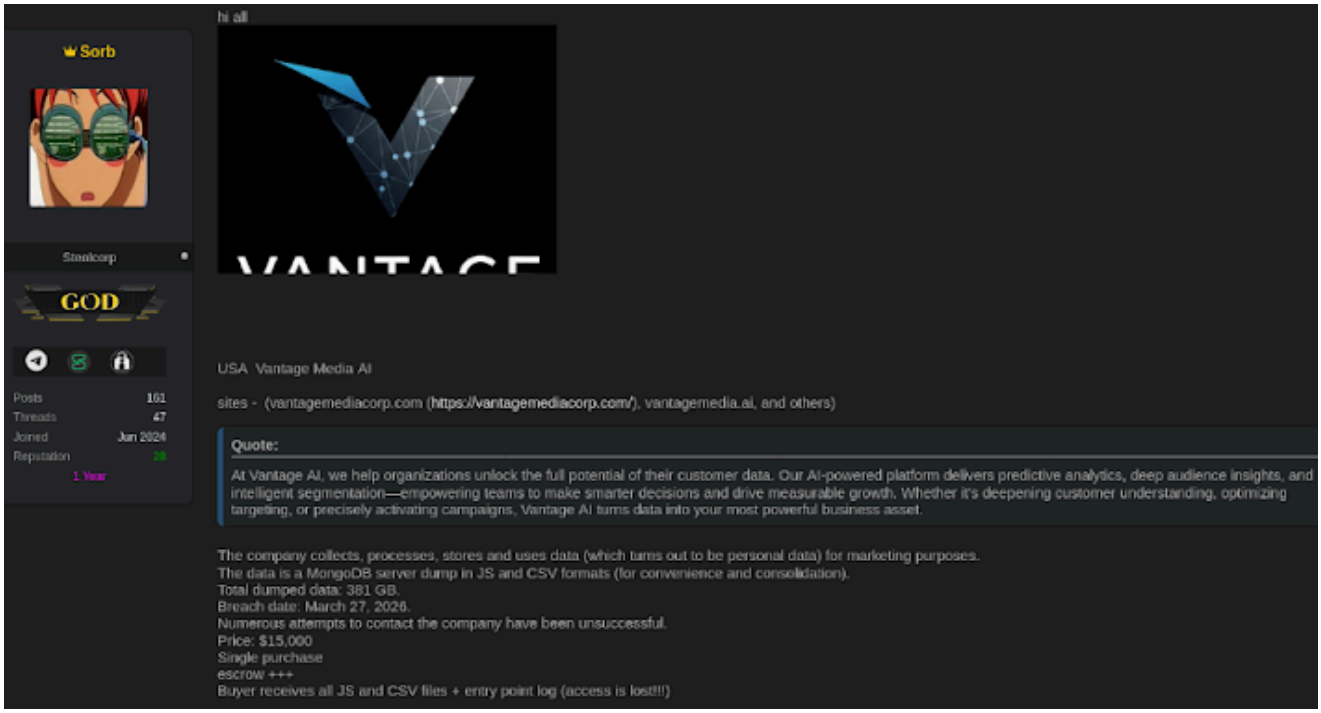
Source: ZeroFox Intelligence

Vespiary claimed that they attempted to contact Vantage Media AI before advertising—very likely as part of an extortion effort—but received no response. It is likely that the failure to extort money from the company directly prompted the actor to advertise the data on the dark web.

- According to the advertisement, the data set also contains CSV and JavaScript files, along with an entry point log that allegedly documents initial access. However, the entry point is no longer accessible, as of writing.
- The inclusion of demographic attributes (such as political affiliation and religion) further increases the risk of tailored disinformation or manipulation campaigns.

The same 381 GB data set was also advertised on the predominantly English-language dark web forums Spear and DarkForums by moderately credible threat actor "Sorb".

- As the TOX ID and Telegram channel provided in the advertisements are identical, Sorb and Vespiary are very likely the same actors or part of the same operation.
- Sorb has a reputation score of 28 on DarkForums, while Vespiary has a reputation score of five on Exploit, suggesting both these accounts are likely considered to be moderately credible.



Sorb's advertisement on DarkForums

Source: ZeroFox Intelligence

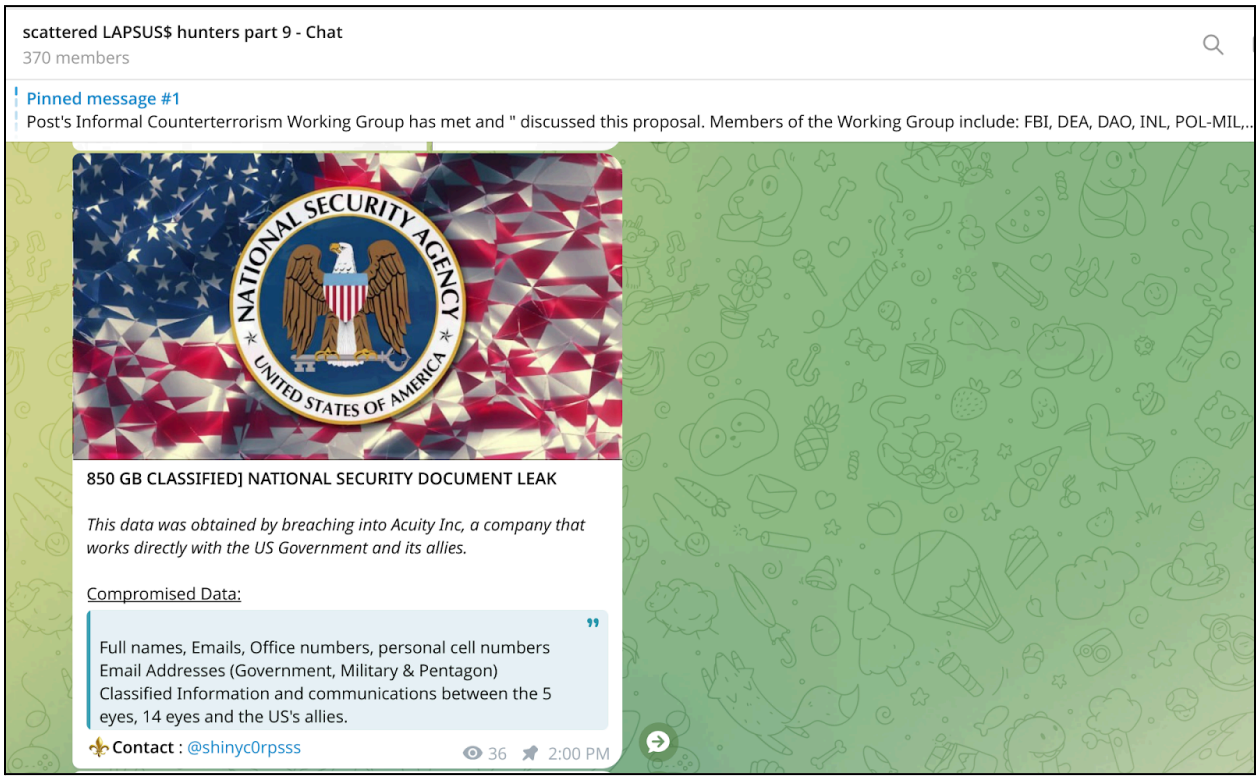
There is a roughly even chance that the claims in the advertisements are true, given the moderately credible reputation of the advertising profiles and the alleged scale of the data included in the leak. Moreover, the price point (USD 15,000 for the entire set) is seemingly lower than what such data sets usually sell for, which is likely to garner more traction from financially motivated threat actors. If true, the leak is very likely to rank among the largest known data exposures, potentially exceeding the scope of the 2021 Facebook data leak, which impacted approximately 533 million users.[2]

Scattered Lapsus$ Hunters Claims Leak of U.S. National Security Documents

On March 31, 2026, threat actor group Scattered Lapsus$ Hunters (SLH) announced on its Telegram channel an alleged 850 GB leak of classified U.S. national security documents. The data was allegedly exfiltrated via a breach of Acuity Inc., a tech consulting firm working with federal agencies. The data set purportedly includes PII; email addresses of government, military, and Pentagon offices; and "classified information" involving the Five Eyes and other U.S. allies. SLH said the price would be disclosed upon contact.

- Acuity Inc. describes itself as a technology consulting firm based in Reston, Virginia.[3] In March 2026, Acuity Inc. announced that it had been selected on a major contract for the Department of State.[4]

[2] hXXps://www.theguardian[.]com/technology/2021/apr/03/500-million-facebook-users-website-hackers
[3] hXXps://www.linkedin[.]com/company/acuity-inc
[4] hXXps://myacuity[.]com/2026/03/26/acuity-awarded-federal-contract-vehicle-evolve-idiq-to-support-department-of-state-enterprise-it-services/



Advertisement on the SLH Telegram channel

Source: ZeroFox Intelligence

The recent SLH leaked data set is almost certainly recycled, as the sample provided is identical to a BreachForums advertisement posted by the well-regarded threat actor IntelBroker (now arrested) on April 2, 2024.[5][6] Since April 2024, multiple users on various dark web forums have reposted the same data set. However, the legitimacy of the 2024 data set remains unknown.

[5] hXXps://cloud.zerofox.com/intelligence/advanced_dark_web/61799

[6] hXXps://www.justice[.]gov/usao-sdny/pr/serial-hacker-intelbroker-charged-causing-25-million-damages-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%

Appendix C: ZeroFox Intelligence Threat Actor Reputation Scale

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