ZEROFOX INTELLIGENCE

Brief

The Underground Economist: Volume 5, Issue 21

B-2025-10-23b

Classification: TLP:CLEAR

Criticality: LOW

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

October 23, 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 23, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Brief | The Underground Economist: Volume 5, Issue 21

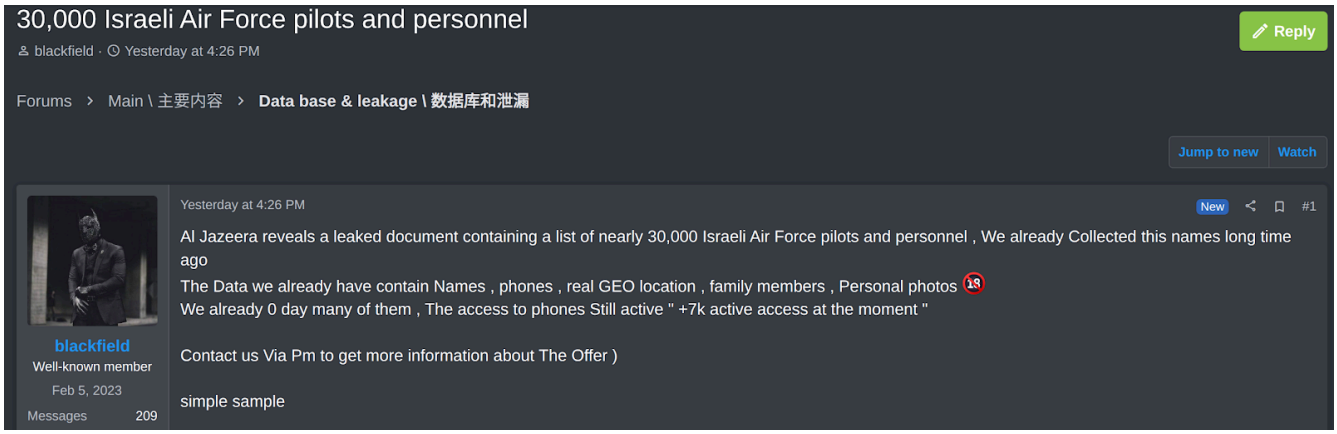
| PII Related to Israeli Air Force Personnel Advertised for Sale on Dark Web

On October 21, 2025, notorious threat actor "blackfield" posted in the dark web forum RAMP, claiming to have collected the personally identifiable information (PII) of 30,000 Israeli Air Force personnel that was recently referenced in a Qatari Al Jazeera broadcast. No pricing was provided in the post; however, blackfield invited interested parties to contact them via private message for more information.

- Blackfield alleged that they had previously collected the PII, which was referenced in a Qatari Al Jazeera broadcast on October 20, 2025, titled "'The Hidden is More Immense"; the network claimed to have obtained a "leaked document" containing the names of approximately 30,000 Israeli Air Force personnel.[1]
- Blackfield is part of the pro-Palestinian, anti-Israel hacktivist group Shadow, a collective responsible for numerous cyberattacks exclusively targeting Israeli infrastructure.
- Blackfield joined RAMP on February 5, 2023, where they have a "well-known member" reputation status.
- On March 15, 2025, blackfield announced on RAMP that they had gained access to sensitive documents associated with high-ranking Israeli Defense Forces (IDF)

[1] hXXps://vinnews[.]com/2025/10/21/al-jazeera-airs-alleged-leak-of-30000-israeli-air-force-personnel/

officers, Israeli political figures, and an Israel-based healthcare organization with an annual revenue of USD 1 billion.



blackfield's RAMP post

Source: ZeroFox Intelligence

In the post, blackfield claims to have collected the information a "long time ago", although no specific timeframe was provided. They also have allegedly compromised at least 7,000 active phone numbers belonging to the military personnel mentioned using an unspecified zero-day vulnerability. The dataset allegedly contains:

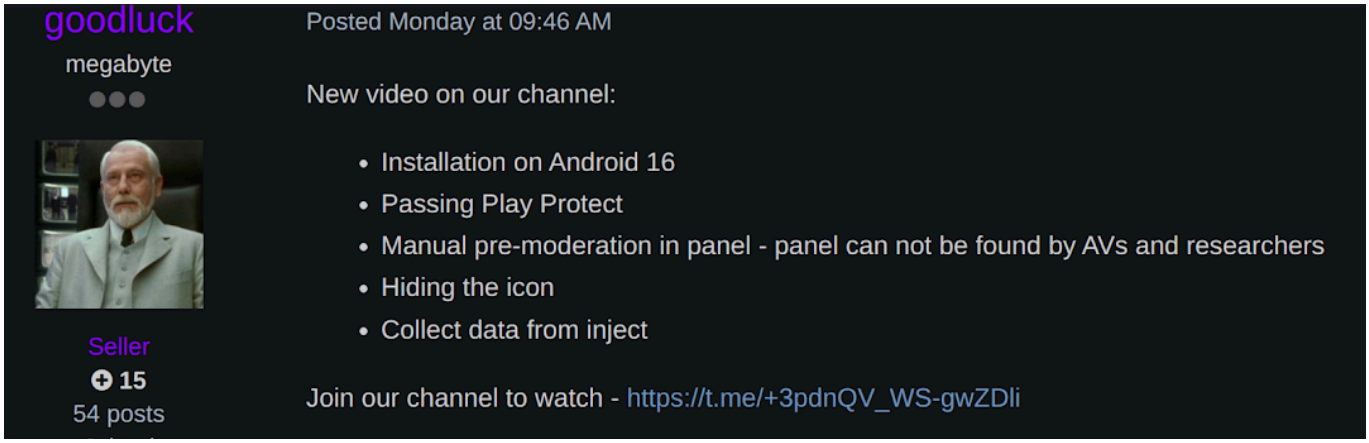
- Names
- Phone numbers
- Geolocation data (likely pertaining to residential addresses)
- Family member information (likely pertaining to names and residential addresses)
- Personal photographs

The dataset advertised is very likely genuine, based on blackfield's established reputation and similar past advertisements. The information advertised by blackfield almost certainly appeals primarily to other ideologically, politically, and financially motivated threat actors that would seek to leverage PII in disruption attacks, social engineering campaigns, or in the planning of physical targeting.

Updates to Octo Bot Posted in Dark Web Forum

On October 20, 2025, an actor using the alias “goodluck” posted in the dark web forum Exploit regarding well-known Android malware bot “Octo”, announcing their latest updates for “Octo 2” and revealing license prices of USD 2,000 for two weeks or USD 3,000 for one month. The actor also shared GitHub documentation for Octo 2, likely to provide proof of authenticity to interested buyers.[2]

- Octo 2 is one of the most advanced and commonly used Android bots and is capable of stealing data via private and customized injections.
- One of the updated bot’s most notable features is its hidden virtual network computing (HVNC) capability, which enables the attacker to remotely control the infected device without the victim’s knowledge.
- On August 20, 2024, goodluck announced the release of the new version of their Octo malware, Octo 2; now, the associated bot has been updated.



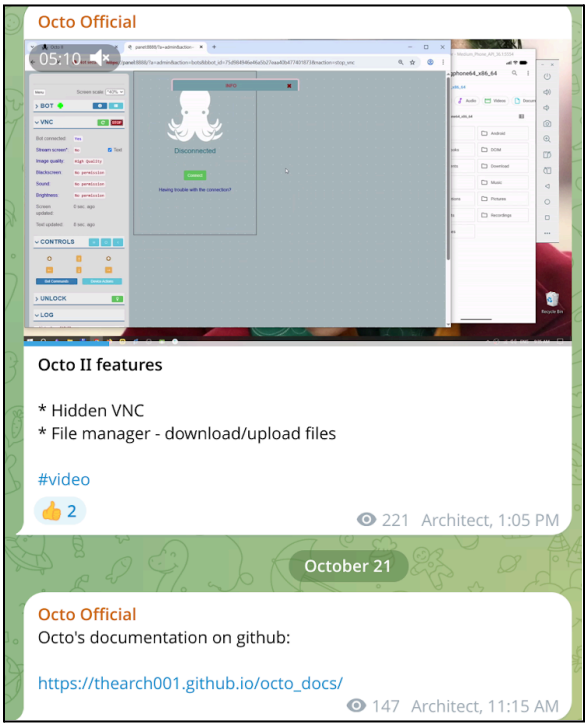
goodluck’s Exploit post

Source: ZeroFox Intelligence

[2] hXXps://thearch001.github[.]io/octo_docs/

The actor goodluck claims in the post that the new Octo 2 bot features include:

- **Compatibility with Android 16:** This indicates the bot functions with a newer operating system (OS) for Android devices, which likely adapted the bot to newer OS APIs and protections to increase the number of vulnerable victims.
- **Ability to bypass Google Play Protect:** This likely means that the bot can bypass Google Play Protect's scanning and blocking mechanisms.
- **Manual pre-moderation in the control panel:** The actor asserts that control-panel submissions are manually reviewed and that the panel has been improved to evade detection by some AV vendors or researchers.
- **Hiding the app icon**: This likely means that the bot can remove its launcher icon so the app is not visible in the application grid, making it less likely that a user will notice and manually uninstall it.
- **Collection of data from injections:** This likely refers to the use of UI overlaps or app-injection techniques to intercept credentials, session tokens, messages, or other sensitive information from targeted apps or web content.



goodluck's Telegram posts

Source: ZeroFox Intelligence

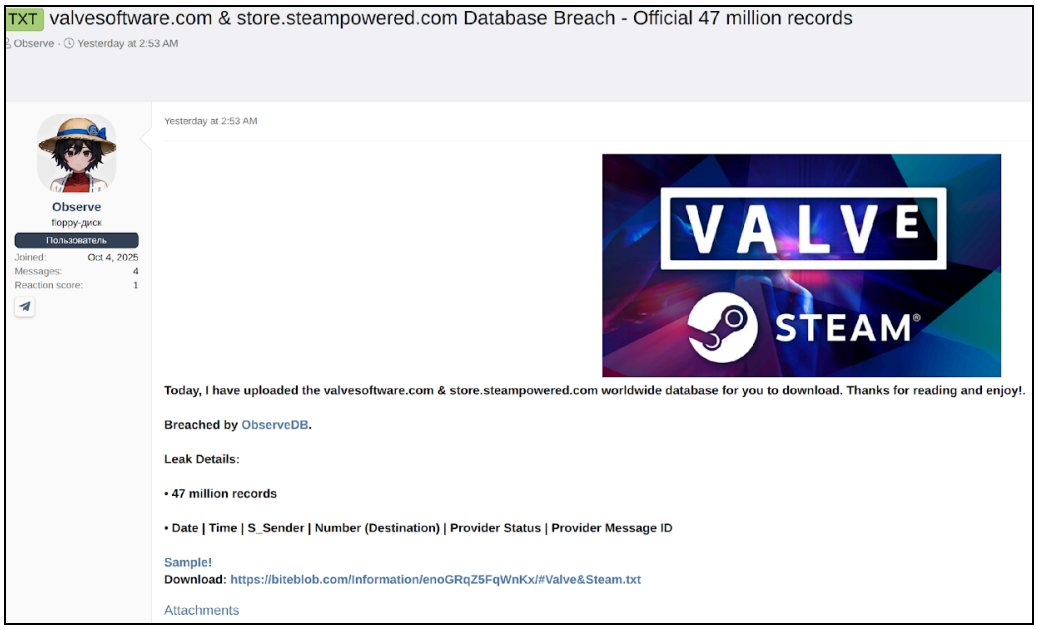
These most recent updates likely represent an attempt by goodluck to promote the Octo 2 bot to attract more users and gain more market share. The updates are likely also aimed at increasing the potential victim pool, especially across devices updated to the newest Android OS. The Octo 2 bot's adaptability and concealment features will likely appeal to buyers and increase the likelihood it will remain one of the most commonly purchased bots on the market.

Database Related to Valve and Steam Advertised for Download on Dark Web Forum

On October 13, 2025, a threat actor using the alias "Observe" posted in the dark web forum XSS, advertising a database for download related to valvesoftware[.]com and store.steampowered[.]com. Observe stated in the post that the database contains approximately 47 million records, which the actor claimed to have personally breached; if true, this would likely indicate the data is recent and not recycled.

- Valve Corporation, commonly referred to as Valve Software, is an American company based in Bellevue, Washington, that specializes in video game development, publishing, and digital distribution.
- The website, store.steampowered[.]com, is Valve Corporation's official digital storefront for PC games, allowing users to browse, purchase, and download titles from both independent developers and major publishers.[3]
- Observe joined XSS on October 4, 2025, and has not yet established a positive reputation. Therefore, ZeroFox cannot determine Observe's credibility at this time.

[3] hXXps://www.valvesoftware[.]com/en/about



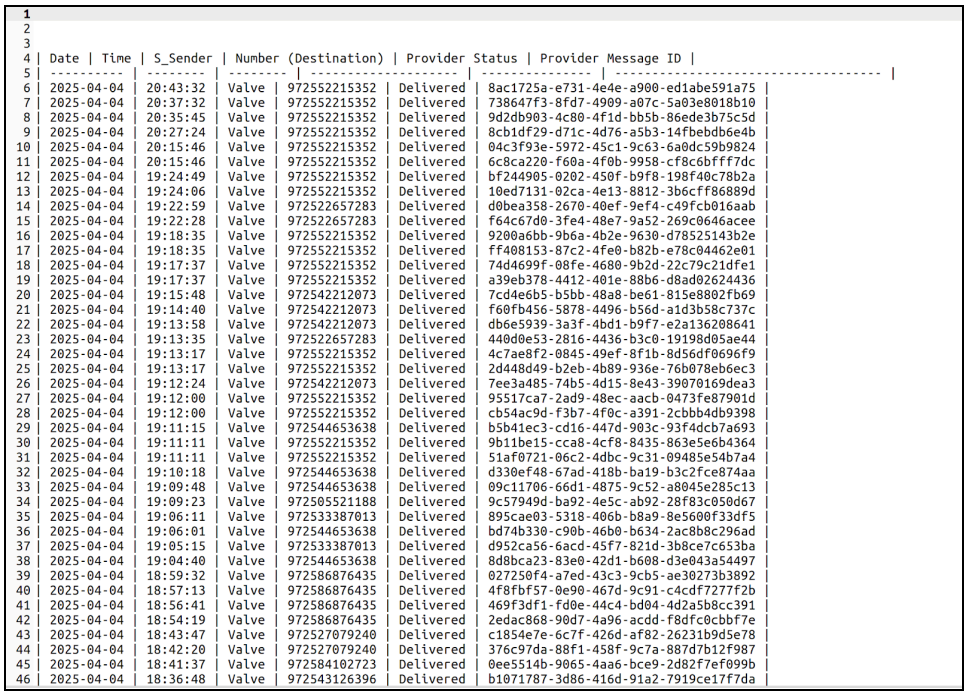
Observe's XSS post

Source: ZeroFox Intelligence

In the post, Observe included the following field headers:

Field	Likely meaning
Date	The calendar date of an event or transaction
Time	The exact time the event occured
S_Sender	The component or service that sent the message
Number (Destination)	The Phone number or destination identifier for an SMS, Steam account IDS, or user identifier
Provider Status	The delivery status reported by the message provider
Provider Message ID	A unique identifier assigned by the provider to each message sent

Observe provided a sample of the database stored in a 38 KB file, which included similar data headers as listed in the table above. The actor also claimed that the full database had been uploaded but did not provide a download link to the complete dataset.



Date	Time	S_Sender	Number (Destination)	Provider Status	Provider Message ID
2025-04-04	20:43:32	Valve	972552215352	Delivered	8ac1725a-e731-4e4e-a900-ed1abe591a75
2025-04-04	20:37:32	Valve	972552215352	Delivered	738647f3-8fd7-4909-a07c-5a03e8018b10
2025-04-04	20:35:45	Valve	972552215352	Delivered	9d2db903-4c80-4f1d-bb5b-86ede3b75c5d
2025-04-04	20:27:24	Valve	972552215352	Delivered	8cb1df29-d71c-4d76-a5b3-14fbebdb6e4b
2025-04-04	20:15:46	Valve	972552215352	Delivered	04c3f93e-5972-45c1-9c63-6a0dc59b9824
2025-04-04	20:15:46	Valve	972552215352	Delivered	6c8ca220-f60a-4f0b-9958-cf8c6bfff7dc
2025-04-04	19:24:49	Valve	972552215352	Delivered	bf244905-0202-450f-b9f8-198f40c78b2a
2025-04-04	19:24:06	Valve	972552215352	Delivered	10ed7131-02ca-4e13-8812-3b6cff86889d
2025-04-04	19:22:59	Valve	972522657283	Delivered	d0bea358-2670-40ef-9ef4-c49fcb016aab
2025-04-04	19:22:28	Valve	972522657283	Delivered	f64c67d0-3fe4-48e7-9a52-269c0646acee
2025-04-04	19:18:35	Valve	972552215352	Delivered	9200a6bb-9b6a-4b2e-9630-d78525143b2e
2025-04-04	19:18:35	Valve	972552215352	Delivered	ff408153-87c2-4fe0-b82b-e78c04462e01
2025-04-04	19:17:37	Valve	972552215352	Delivered	74d4699f-08fe-4680-9b2d-22c79c21dfe1
2025-04-04	19:17:37	Valve	972552215352	Delivered	a39eb378-4412-401e-88b6-d8ad02624436
2025-04-04	19:15:48	Valve	972542212073	Delivered	7cd4e6b5-b5bb-48a8-be61-815e8802fb69
2025-04-04	19:14:40	Valve	972542212073	Delivered	f60fb456-5878-4496-b56d-a1d3b58c737c
2025-04-04	19:13:58	Valve	972542212073	Delivered	db6e5939-3a3f-4bd1-b9f7-e2a136208641
2025-04-04	19:13:35	Valve	972522657283	Delivered	440d0e53-2816-4436-b3c0-19198d05ae44
2025-04-04	19:13:17	Valve	972552215352	Delivered	4c7ae8f2-0845-49ef-8f1b-8d56df0696f9
2025-04-04	19:13:17	Valve	972552215352	Delivered	2d448d49-b2eb-4b89-936e-76b078eb6ec3
2025-04-04	19:12:24	Valve	972542212073	Delivered	7ee3a485-74b5-4d15-8e43-39070169dea3
2025-04-04	19:12:00	Valve	972552215352	Delivered	95517ca7-2ad9-48ec-aacb-0473fe87901d
2025-04-04	19:12:00	Valve	972552215352	Delivered	cb54ac9d-f3b7-4f0c-a391-2cbbb4db9398
2025-04-04	19:11:15	Valve	972544653638	Delivered	b5b41ec3-cd16-447d-903c-93f4dcb7a693
2025-04-04	19:11:11	Valve	972552215352	Delivered	9b11be15-cca8-4cf8-8435-863e5e6b4364
2025-04-04	19:11:11	Valve	972552215352	Delivered	51af0721-06c2-4dbc-9c31-09485e54b7a4
2025-04-04	19:10:18	Valve	972544653638	Delivered	d330ef48-67ad-418b-ba19-b3c2fce874aa
2025-04-04	19:09:48	Valve	972544653638	Delivered	09c11706-66d1-4875-9c52-a8045e285c13
2025-04-04	19:09:23	Valve	972505521188	Delivered	9c57949d-ba92-4e5c-ab92-28f83c050d67
2025-04-04	19:06:11	Valve	972533387013	Delivered	895cae03-5318-406b-b8a9-8e5600f33df5
2025-04-04	19:06:01	Valve	972544653638	Delivered	bd74b330-c90b-46b0-b634-2ac8b8c296ad
2025-04-04	19:05:15	Valve	972533387013	Delivered	d952ca56-6acd-45f7-821d-3b8ce7c653ba
2025-04-04	19:04:40	Valve	972544653638	Delivered	8d8bca23-83e0-42d1-b608-d3e043a54497
2025-04-04	18:59:32	Valve	972586876435	Delivered	027250f4-a7ed-43c3-9cb5-ae30273b3892
2025-04-04	18:57:13	Valve	972586876435	Delivered	4f8fbf57-0e90-467d-9c91-c4cdf7277f2b
2025-04-04	18:56:41	Valve	972586876435	Delivered	469f3df1-fd0e-44c4-bd04-4d2a5b8cc391
2025-04-04	18:54:19	Valve	972586876435	Delivered	2edac868-90d7-4a96-acdd-f8dfc0cbbf7e
2025-04-04	18:43:47	Valve	972527079240	Delivered	c1854e7e-6c7f-426d-af82-26231b9d5e78
2025-04-04	18:42:20	Valve	972527079240	Delivered	376c97da-88f1-458f-9c7a-887d7b12f987
2025-04-04	18:41:37	Valve	972584102723	Delivered	0ee5514b-9065-4aa6-bce9-2d82f7ef099b
2025-04-04	18:36:48	Valve	972543126396	Delivered	b1071787-3d86-416d-91a2-7919ce17f7da

Sample database shared by Observe

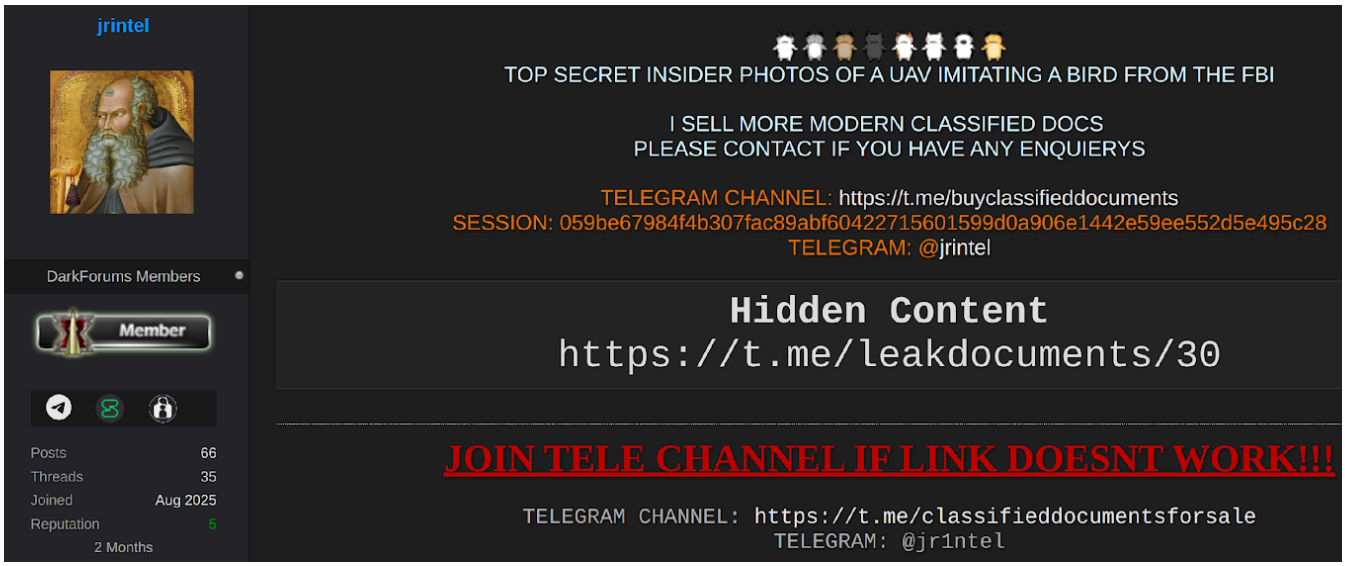
Source: ZeroFox Intelligence

It is very likely that Observe is attempting to build credibility and garner attention on the forum by claiming responsibility for disclosing such a large dataset. By posting a sample of the data and omitting the full download, it is likely that Observe is attempting to generate interest before selling the full dataset. The data, if legitimate, will likely appeal to a variety of threat actors seeking to conduct malicious cyber campaigns, such as social engineering or phishing.

Top Secret Information Related to the FBI Advertised for Sale on Dark Web Forum

On October 8, 2025, an actor using the alias “jrintel” posted in the dark web forum DarkForums, advertising the sale of top secret U.S. Federal Bureau of Investigation (FBI) schematics of an unmanned aerial vehicle (UAV) designed to imitate a bird. The actor did not disclose a price for the alleged documentation but provided Telegram and Session links for any interested parties to use to contact them.

- Jrintel joined DarkForums in August 2025 and has since garnered a positive reputation, which likely adds credibility to their claims.



jrintel's DarkForums post

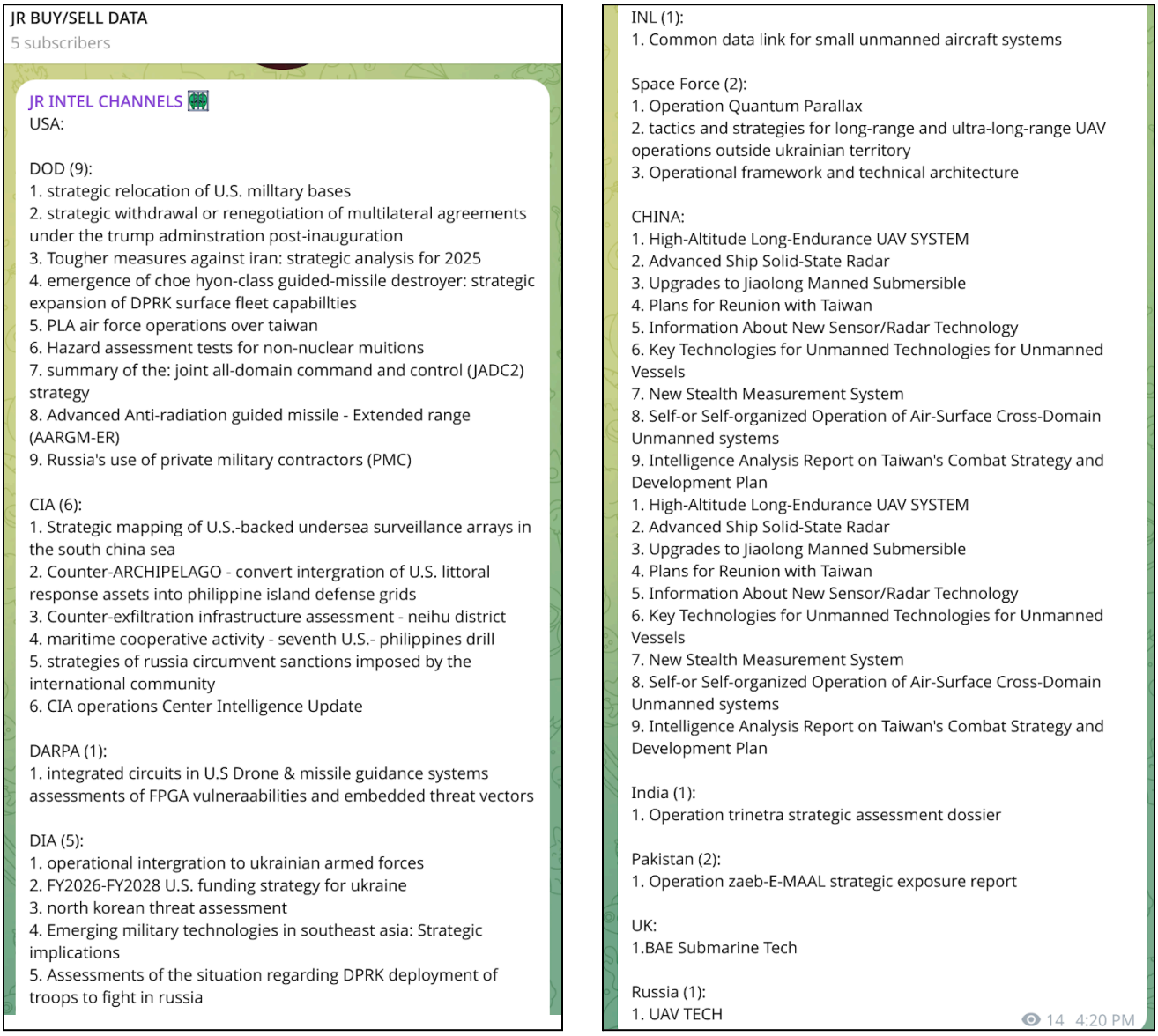
Source: ZeroFox Intelligence

In the post, jrintel provided a Telegram link[4] to access the content—likely to showcase proof of the documentation; however, the channel has since been removed or deleted by the owner. Jrintel operates a separate Telegram channel called "buygovdocs"[5] where they frequently advertise the purchase and sale of sensitive worldwide government-related information. In this channel—which was established on October 13, 2025, just five days after the actor's most recent UAV schematics offer—jrintel shared a list of alleged material that they claim to possess, including documentation related to the following governments:

- The United States: Information related to the Department of War (DoW), the Central Intelligence Agency (CIA), the Defense Advanced Research Projects Agency (DARPA), the Defense Intelligence Agency (DIA), the Idaho National Laboratory, and Space Force
- China: Information related to UAVs and strategic plans for Taiwan
- India: A strategic assessment on "Operation Trinetra"

[4] hXXps://t[.]me/leakdocuments/30
[5] hXXps://t[.]me/buygovdocs

- Pakistan: A strategic report on “Operation Zeb-e-Maal”
- United Kingdom: BAE Systems submarine technology developments
- Russia: UAV technology advancements



Alleged material leaked on the “buygovdocs” Telegram channel

Source: ZeroFox Intelligence

It is likely that the advertisement posted by jrintel on DarkForums is credible, given their positive reputation on the forum. There is a likely chance that jrintel is in possession of at

least some of the documentation that they advertised on their "buygovdocs" Telegram channel as well. The information that jrintel claims to be in possession of is likely to appeal to both financially motivated threat actors—who would likely seek to sell the data to nation-states or the media—and nation-states seeking to obtain information on governments they perceive to be adversarial.

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 deep and dark web (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%