ZEROFOX INTELLIGENCE

# Brief

## The Underground Economist: Volume 5, Issue 23

B-2025-11-21a

Classification: TLP:CLEAR

Criticality: LOW

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

November 20, 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 (EST) on November 20, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

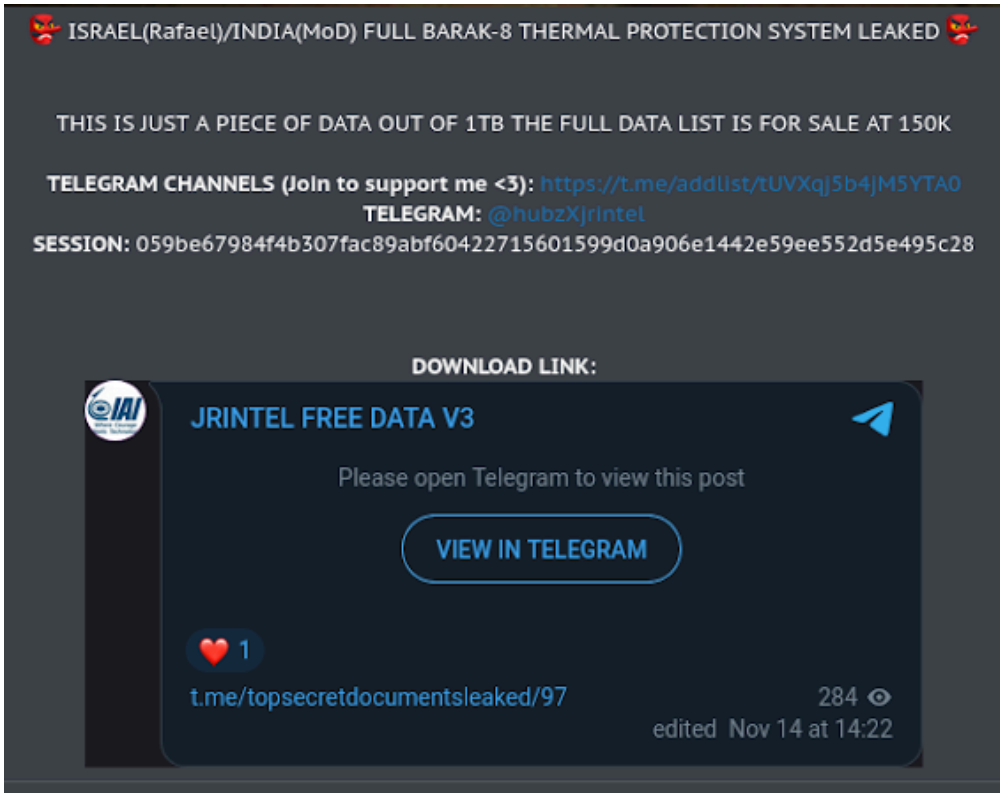
# | Brief | The Underground Economist: Volume 5, Issue 23

## | Documents Related to Israeli Military Advertised for Sale on Dark Web Forum

On November 15, 2025, reputable threat actor "jrintel" advertised the sale of a 1 TB file set allegedly related to Barak-8 (a missile system used by Israel) on the dark web forum ReHub. The leak purportedly includes source code, DWG files (binary file format that stores two- and three-dimensional design data), documents, photos, and videos for the thermal protection system. The actor's asking price for the complete dataset is USD 150,000.

- Barak-8 is a long-range surface-to-air missile (LR-SAM) system that was jointly developed by Israel and India and is used by their militaries.
- ReHub is a dark web forum that was established by actor "ReHub", a former moderator for the dark web forums XSS and RAMP. Jrintel joined ReHub on November 9, 2025.
- On October 8, 2025, jrintel posted in the dark web forum DarkForums, advertising the sale of allegedly 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 for distributing leaked, sensitive, government-related documents and information.

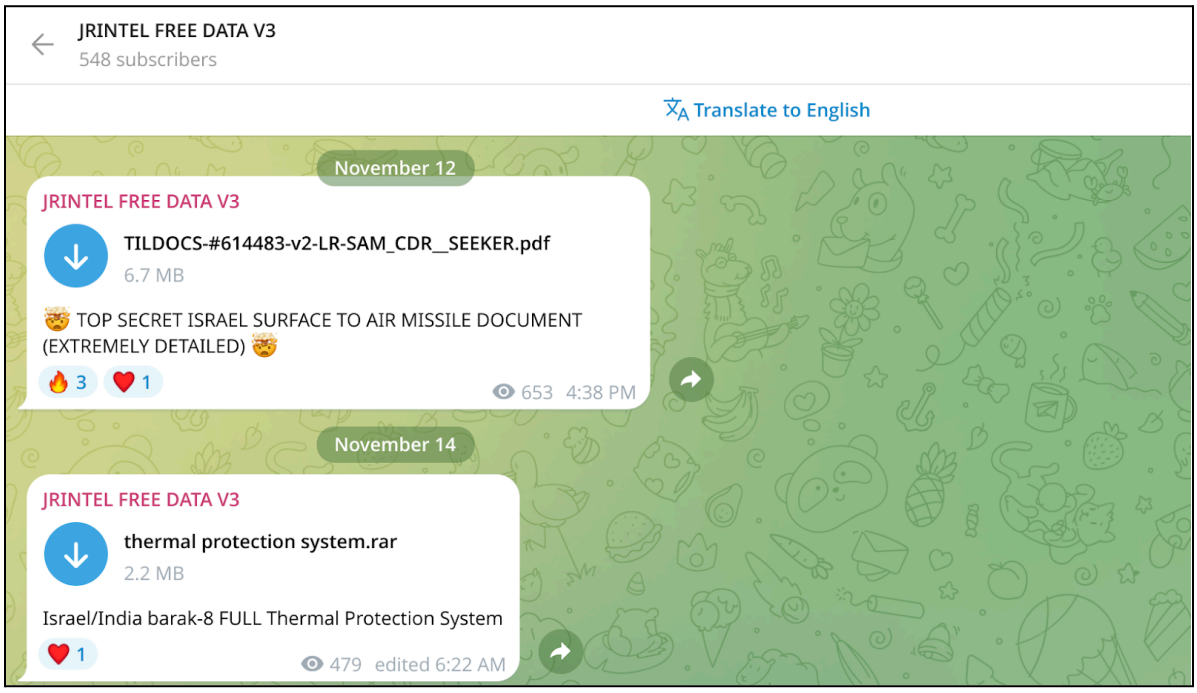



**jrintel's ReHub post**
*Source: ZeroFox Intelligence*

Jrintel operates a Telegram channel (which they provided a link to in the post for purposes of downloading the free sample data[1]), where they share samples of the leaked material. In addition to samples from the alleged Barak-8 leak, jrintel has also posted samples allegedly tied to a separate Israeli surface-to-air missile (SAM) system. ZeroFox obtained both sample packs and assesses the documents are likely authentic based on our initial review.

[1] hXXps://t[.]me/topsecretdocumentsleaked

- In a previous post on October 8, 2025, jrintel provided a different Telegram link[2] to access the content—likely to showcase proof of the documentation—however, the channel has since been removed or deleted by the owner.




**Alleged material leaked on the "topsecretdocumentsleaked" Telegram channel**

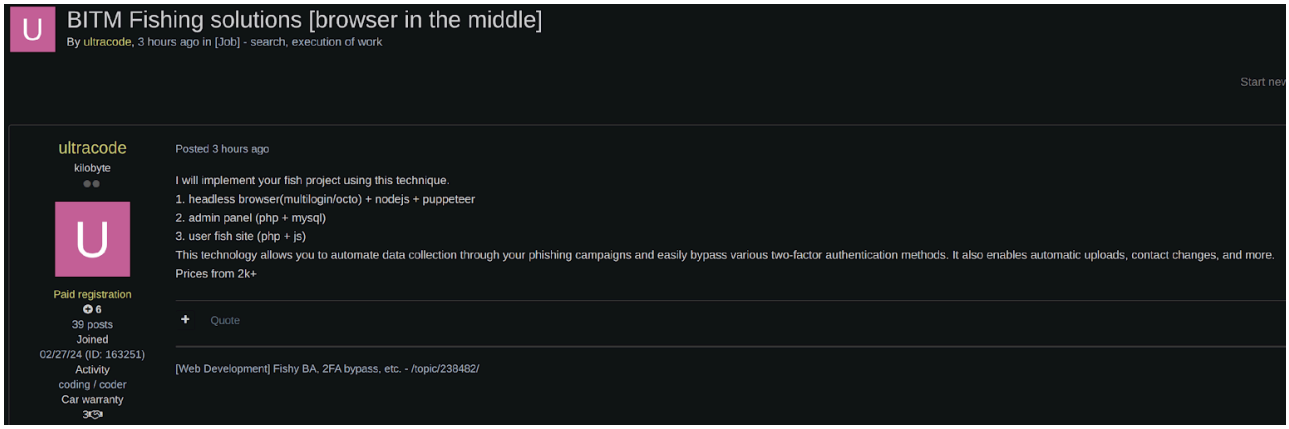
*Source: ZeroFox Intelligence*

It is likely that the advertisement posted by jrintel on ReHub is credible, given their positive reputation on DarkForums. 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.

[2] hXXps://t[.]me/leakdocuments/30

# Browser in the Middle Phishing Solution Available on DarkNet

On November 11, 2025, an actor using the alias “ultracode” on the dark web forum Exploit advertised a custom implementation technique for phishing campaigns using what they described as a browser in the middle (BITM) solution. The service has a listing price of at least USD 2,000.




**ultracode’s original Exploit post**
*Source: ZeroFox Intelligence*

According to the listing, the approach combines:

- A headless browser environment, which is very likely to improve evasion of security analysis;
- An administrative backend (PHP/MySQL), likely for centralized campaign management; and.
- A client-supplied phishing site, almost certainly to improve customization without the need for technical skills.

Ultracode claims the technology automates credential harvesting and can bypass various two-factor authentication measures; they also promoted features such as automatic uploads and contact changes, though these were not specified in detail.

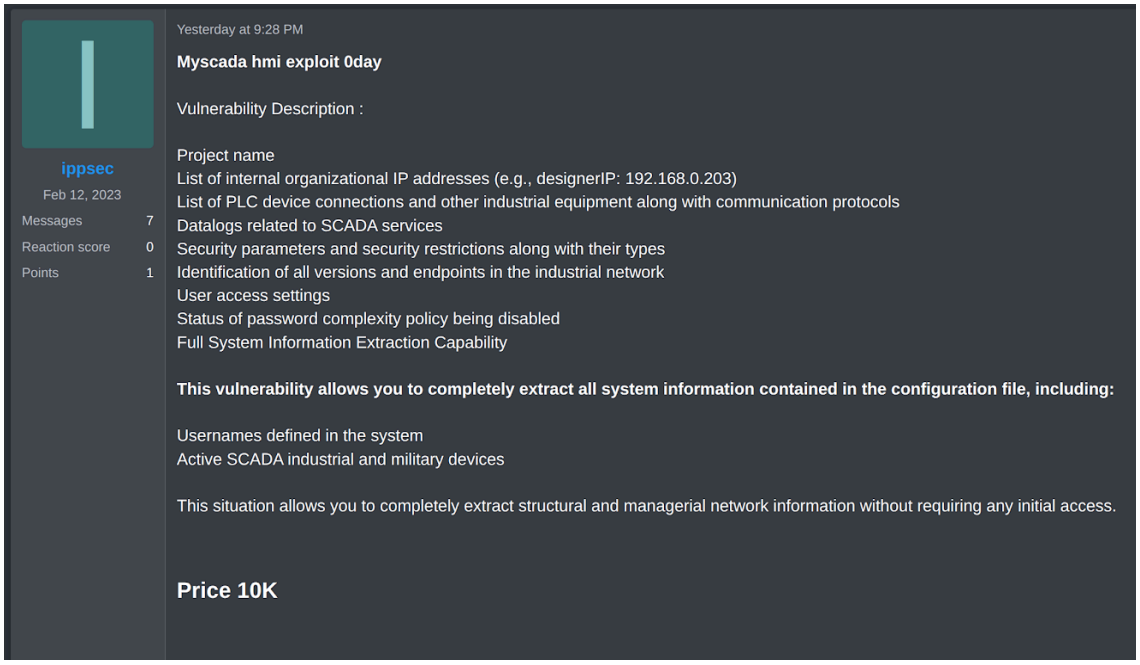
ZeroFox assesses that, while the concept appears plausible in theory, it is very likely untested based on current observations. However, a functioning BITM solution would

almost certainly enable more efficient, large-scale phishing campaigns that require fewer resources than traditional bot-only approaches.

## RAMP Actor Advertises Alleged MySCADA HMI Zero-Day Exploit

On November 10, 2025, low-reputation threat actor "ippsec" advertised a "MyScada HMI" zero-day exploit on the dark web forum RAMP. Ippsec claimed the exploit can extract full system configuration and credentials from affected devices and priced it at USD 10,000.

- MyScada is a Supervisory Control and Data Acquisition (SCADA) and Human-Machine Interface (HMI) system developed by the Czech company mySCADA Technologies. The system is designed to provide visualization, data logging, and control of industrial processes.
- The actor ippsec joined RAMP in 2023 but has a zero reaction score and appears to be largely inactive on the platform.
- As of writing, the post has garnered some attention, with other RAMP members advising ippsec and their potential buyers to use escrow services during the purchase process (a common practice on dark web forums that serves to ensure payment and reduce the risk of fraud among cybercriminals).




**ippsec's RAMP post**

*Source: ZeroFox Intelligence*

The actor further claimed that the exploit enables full-system information extraction, enabling an attacker to harvest all configuration-stored data without detection. This includes usernames and other sensitive operational details for active SCADA and, reportedly, military-linked devices.

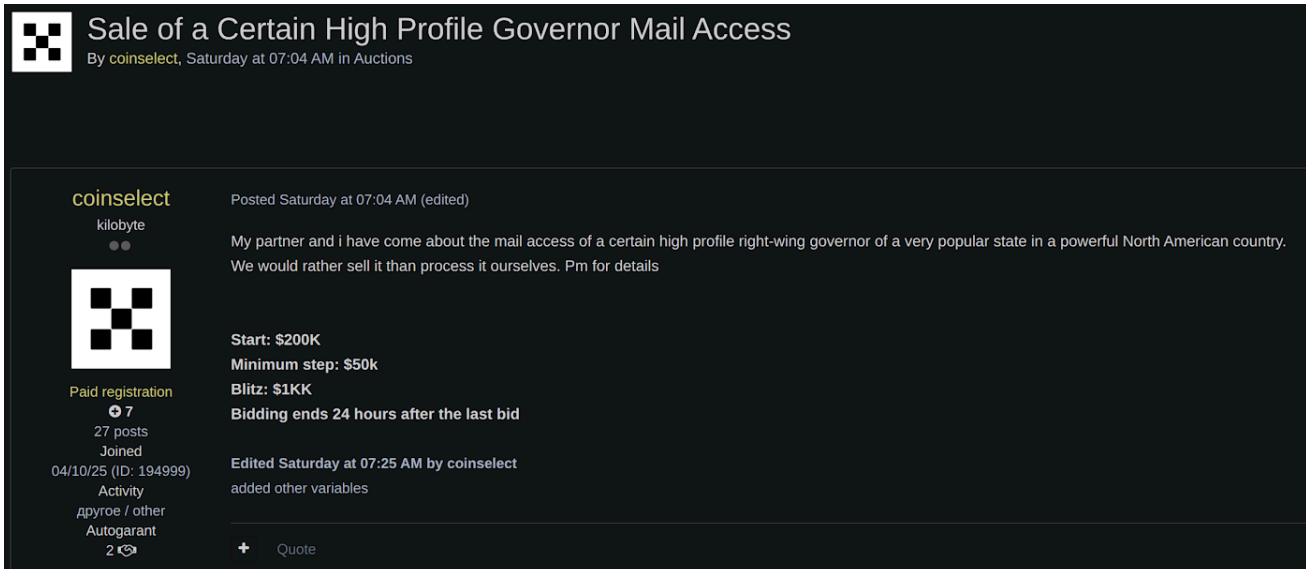
- The exploit allegedly exposes several categories of sensitive data: internal organizational IP addresses, programmable logic controller (PLC) and industrial device connections with associated communication protocols, and datalogs linked to SCADA service activity.
- The ability to extract full system configuration, internal IPs, PLC mappings, datalogs, and user credentials would likely provide potential buyers with near-total visibility into an industrial network. This level of access has the potential to enable follow-on actions such as credential compromise, unauthorized control of PLCs, and OT network reconnaissance. Such a capability presents high-risk exposure for any affected device.

Given the actor's reputation and the lack of technical proof-of-concept or samples, it is likely they are attempting to build credibility and garner attention on the forum by advertising an exploit that targets the controls of critical infrastructure. If ippsec's claims are legitimate, such access would likely significantly compromise network visibility, authentication security, and operational integrity within affected environments that have not patched this vulnerability.

## California Governor Email Access Advertised for Sale

On November 8, 2025, the actor "coinselect" announced on the Exploit forum that they had obtained email access to a high-profile U.S. governor's account and were offering it for sale at auction. The listing had a starting price of USD 200,000, with a minimum bid increment of USD 50,000—or an immediate purchase price of USD 1 million.

- Coinselect joined Exploit in April 2025 and is considered a vetted member of the forum, indicating the offer of access is likely legitimate.




**coinselect's original Exploit post**
*Source: ZeroFox Intelligence*

Following interactions with coinselect, ZeroFox determined that the access for sale was for California Governor Gavin Newsom. The actor also claimed they had access to a remote desktop protocol (RDP) associated with the account, which they stated would be

sold for an additional fee. At the time of reporting, there were no public bids on the auction.

ZeroFox assesses Governor Newsom's office is likely capable of remediating the access; however, the seller has likely already exfiltrated sensitive data from the compromised email account. Depending on exactly what information was in the governor's email account, this data breach could potentially damage confidential relationships or meetings pertinent to State of California business.

## 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% |