



**| Flash |**

# Iranian Data Leak Advertised on the Dark Web

F-2024-06-10a

**Classification:** TLP:CLEAR

**Criticality:** Low

**Intelligence Requirements:** Deep and Dark Web, Data Leak, Threat Actor,  
Nation-State

**June 10, 2024**

**Scope Note:** 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 9:00 AM (EDT) on June 10, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

## Flash | Iranian Data Leak Advertised on the Dark Web

### › Key Findings

- On June 4, 2024, untested English-speaking actor “irleaks” announced the sale of a large leaked data set pertaining to an independent Iranian government agency, the Hajj and Pilgrimage Organization, on the dark web Onniforums community.
- The leaked data will very likely attract threat collectives with geopolitical or ideological motivations, including hacktivist and state-sponsored groups hostile to Iran. Additionally, financially motivated threat actors, such as ransomware groups, will likely be interested.
- The recent data leak is very likely related to the ongoing Israel-Hamas war, as threat actors likely identify a demand from geopolitically aligned actors for state-related data.
- It is likely that data leaks implicating both Israel and Iran will continue to be advertised by threat actors on dark web forums while the conflict persists.

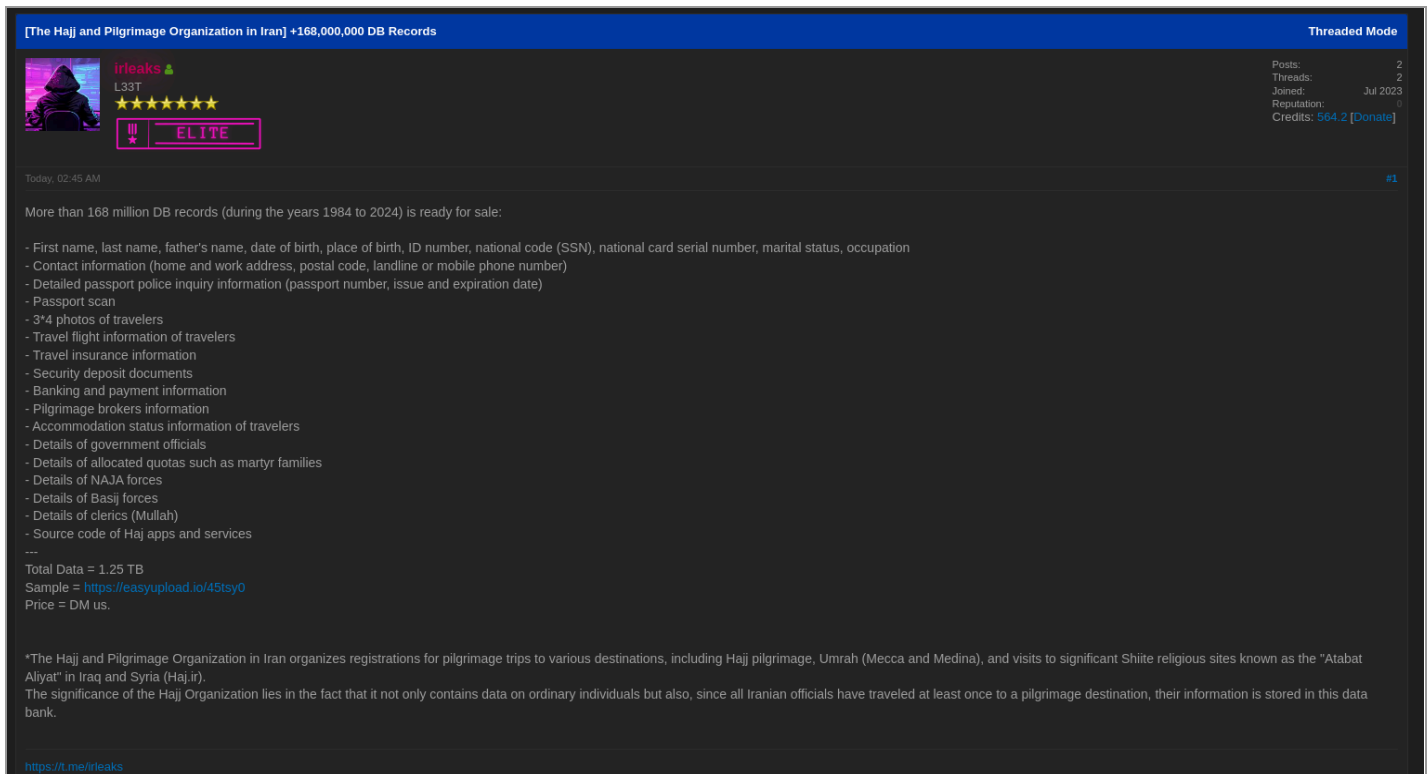
## Details

On June 4, 2024, untested English-speaking actor irleaks announced the sale of a large leaked data set pertaining to the Hajj and Pilgrimage Organization in Iran via the dark web Onniforums community. The data is stated to be substantive, totalling 1.25TB in size and containing over 168 million records spanning from 1984 to 2024. This data will very likely gain the attention of geopolitically and ideologically motivated actors.

- The Hajj and Pilgrimage Organization is an independent government agency in Iran that is responsible for managing and overseeing the Hajj pilgrimage and other religious pilgrimages for all Iranian citizens.
- The price is not specified and is likely a matter of negotiation. However, it is expected to be substantial due to the volume and sensitivity of the leaked data.

The leak allegedly contains a multitude of sensitive data. Additionally, it pertains to information on various organizations and individuals who work with or have used the Hajj and Pilgrimage Organization.

- Allegedly, government officials' information is implicated in the data. These individuals are stated to work with the organization in a government capacity, or the individuals have used the organization in a personal capacity.
- Data pertaining to security forces who cooperate with the agency (such as Iran's national police force, NAJA, and volunteer auxiliary force Basij, which is controlled by the Iranian Armed Forces) is included in the leak.
- Personal financial information such as banking, payment, and pilgrimage broker information is allegedly included, as is personally identifiable information (PII) consisting of contact information, citizen identification, ID data, photos, insurance, and travel information.



The screenshot shows a forum post on OnniForums. The post title is "[The Hajj and Pilgrimage Organization in Iran] +168,000,000 DB Records". The user 'lrleaks' has a profile picture of a person in a hoodie, a level of 'L33T', and a '5★' rating. The post content lists various types of data available for sale, including personal information, travel details, and government records. It also mentions a total data size of 1.25 TB and a price of DM us. The post is marked as 'Threaded Mode' and 'Elite'.

[The Hajj and Pilgrimage Organization in Iran] +168,000,000 DB Records

lrleaks  
L33T  
5★  
ELITE

Today, 02:45 AM

More than 168 million DB records (during the years 1984 to 2024) is ready for sale:

- First name, last name, father's name, date of birth, place of birth, ID number, national code (SSN), national card serial number, marital status, occupation
- Contact information (home and work address, postal code, landline or mobile phone number)
- Detailed passport police inquiry information (passport number, issue and expiration date)
- Passport scan
- 3\*4 photos of travelers
- Travel flight information of travelers
- Travel insurance information
- Security deposit documents
- Banking and payment information
- Pilgrimage brokers information
- Accommodation status information of travelers
- Details of government officials
- Details of allocated quotas such as martyr families
- Details of NAJA forces
- Details of Basij forces
- Details of clerics (Mullah)
- Source code of Haj apps and services

---  
Total Data = 1.25 TB  
Sample = <https://easyupload.io/45tsy0>  
Price = DM us.

\*The Hajj and Pilgrimage Organization in Iran organizes registrations for pilgrimage trips to various destinations, including Hajj pilgrimage, Umrah (Mecca and Medina), and visits to significant Shiite religious sites known as the "Atabat Aliyat" in Iraq and Syria (Hajir).  
The significance of the Hajj Organization lies in the fact that it not only contains data on ordinary individuals but also, since all Iranian officials have traveled at least once to a pilgrimage destination, their information is stored in this data bank.

<https://t.me/lrleaks>

## lrleaks' OnniForums post

Source: ZeroFox Intelligence

While the extent and content of the stolen information is unknown, its quantity and non-public nature means it will very likely be of interest to geopolitically or ideologically motivated threat actors. Therefore, it is very likely that the advertisement is aimed toward hacktivists, state cyber capabilities, and state-affiliated groups that are known to be opposed to Iran. Additionally, financially-motivated threat actors, such as ransomware and digital extortion collectives, will likely be perceived as interested parties.

- Politically motivated actors, such as nation-states and state-sponsored actors, could use the data to target implicated government individuals in social engineering attacks with the intent of conducting espionage.
- Ideologically motivated actors, such as hacktivists, would likely leverage this data to disrupt Iranian organizations using denial-of-service (DoS) attacks or to influence them with information campaigns.
- Financially motivated actors would very likely utilize the data to conduct ransom and digital extortion (R&DE) attacks.

The resurgence of conflict between Israel and Hamas since October 2023 has seen Iran conducting cyberattacks against Israel, while also being the recipient of similar cyberattacks. While Iran has been critical of the approach Israel has taken in the war, Israel has condemned Iran's alleged support of Hamas .

- On March 3, 2024, the pro-Palestinian and English-speaking threat collective "Handala Hack" allegedly gained remote access to Israeli radar systems. On April 13, 2024, the group then announced another breach of the radar systems, which was followed by an Iranian attack.
- The financially and ideologically motivated, pro-Israel hacking collective "R00KIT" claimed responsibility for targeting several Iranian-based organizations and agencies. These targets include a financial exchange system, an educational institution, a hospital, and an overseas logistics company.

The recent data leak is very likely related to the ongoing conflict, as threat actors likely seek to fulfill demand from geopolitically aligned actors for state-related data. Additionally, the leak likely indicates hacktivists and non-hacktivists that are primarily financially motivated are aligning over geo-political events. Therefore, it is likely that data leaks implicating both Israel and Iran will continue to be advertised by threat actors on dark web forums while the Israel-Hamas war persists.

## **Recommendations**

- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Implement secure password policies with phishing-resistant multi-factor authentication (MFA), complex passwords, and unique credentials.
- 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.
- Configure email servers to block emails with malicious indicators and deploy authentication protocols to prevent spoofed emails.
- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process and ensure all IT assets are updated with the latest software updates as quickly as possible.
- Proactively monitor for compromised accounts being brokered in deep and dark web (DDW) forums.
- Configure ongoing monitoring for Compromised Account Credentials.
- 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**

|                                | <b>Red</b>                                                                                                                                                                                             | <b>Amber</b>                                                                                                                                                                                                                                                                                                                 |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>WHEN SHOULD IT BE USED?</b> | <b>Sources may use</b><br><b>TLP:RED</b> 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. | <b>Sources may use</b><br><b>TLP:AMBER</b> when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.                                                                                                           |
| <b>HOW MAY IT BE SHARED?</b>   | <b>Recipients may NOT share</b><br><b>TLP:RED</b> with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.                                     | <b>Recipients may ONLY share</b><br><b>TLP:AMBER</b> 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.<br><b>Note that</b><br><b>TLP:AMBER+STRICT</b> restricts sharing to the organization only. |
|                                | <b>Green</b>                                                                                                                                                                                           | <b>Clear</b>                                                                                                                                                                                                                                                                                                                 |
| <b>WHEN SHOULD IT BE USED?</b> | <b>Sources may use</b><br><b>TLP:GREEN</b> when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.              | <b>Sources may use</b><br><b>TLP:CLEAR</b> when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.                                                                                                                                                      |
| <b>HOW MAY IT BE SHARED?</b>   | <b>Recipients may share</b><br><b>TLP:GREEN</b> information with peers and partner organizations within their sector or community but not via publicly accessible channels.                            | <b>Recipients may share</b><br><b>TLP:CLEAR</b> 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%         |