Iranian Food Delivery Giant Snappfood Cyber Attack: 3TB of Data Stolen

hackread.com/iranian-food-delivery-snappfood-cyber-attack/

January 2, 2024

A hacker or hacker group, identified as “irleaks” (presumably indicating Iran Leaks), publicly disclosed the Snappfood cyber attack on Breach Forums and Telegram over New Year’s Eve.

Snappfood, a prominent online food delivery service in **Iran**, has fallen victim to a major data breach, during which cybercriminals stole personal information of millions of customers, Hackread.com can confirm.

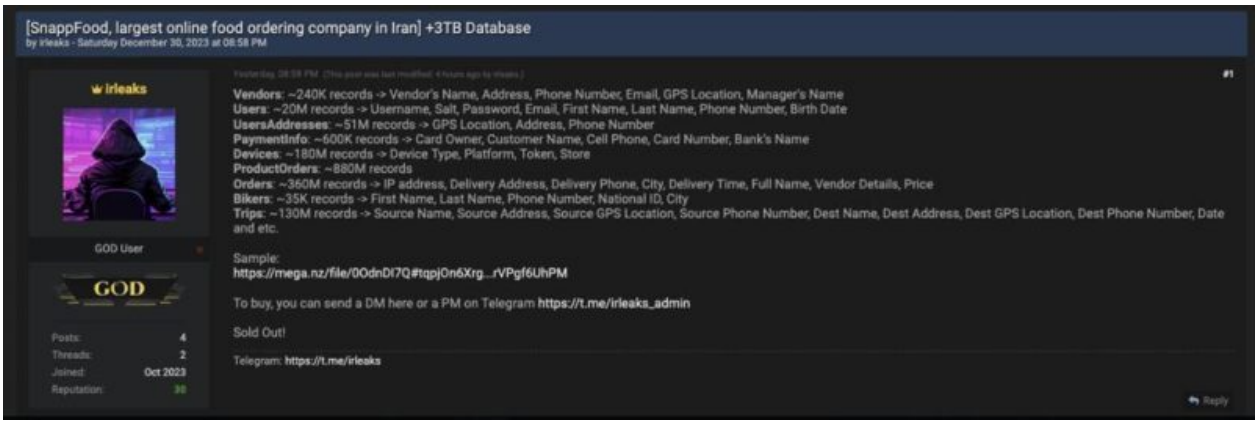
Operating similarly to other food delivery platforms, Snappfood facilitates users in Iran to conveniently order food from a diverse range of restaurants through its mobile app or website, subsequently having it delivered to their doorstep. It forms part of the larger Snapp group, which includes Snapp’s ride-hailing services.

In the wake of this data breach, an individual operating under the alias “irleaks” (presumably indicating Iran Leaks) publicly disclosed a sample of the stolen data on the notorious **Breach Forums**, indicating the specifics of the compromised information.

As seen by Hackread.com, the hacker claimed to have acquired an extensive trove of data exceeding 3TB. Allegedly, the stolen records include:

1. **Customer Information:** Details of over 20 million customers, including usernames, password hashes, email addresses, full names, dates of birth, and phone numbers.
2. **Vendor Records:** Records of 240,000 vendors, featuring names, addresses, phone numbers, email addresses, GPS locations, and managers’ names.
3. **Payment Information:** Payment details of over 600,000 customers, incorporating card owner names, customer full names, phone numbers, card numbers, and bank names.
4. **Device Data:** Data from 180 million devices, including device types, platforms, tokens, and store names.
5. **Product Orders:** The hacker alleges to have accessed more than 880 million product order records.
6. **Orders:** Apparently, 360 million order details, encompassing IP addresses, delivery addresses, delivery phone numbers, city, time, customer full names, vendor details, and prices, were compromised.
7. **Biker/Rider Details:** The breach also affected the details of the bikers or riders responsible for order delivery, with 35,000 records, including full names, phone numbers, national ID card details, and cities, being stolen.

8. **Trip Details:** The breach allowed “irleaks” to extract trip-related information, comprising 130 million records containing source names, addresses, GPS locations, phone numbers, destinations, and addresses.



irleaks’ post on Breach Forums (Screenshot credit: Hackread.com)

Snappfood Acknowledges the Data Breach

While the official Snappfood Iran website was inaccessible at the time of writing this article, on December 31, 2023, the company publicly acknowledged the breach on Twitter (now X), acknowledging the issue. Snappfood’s social media representative disclosed that Iran’s Cyber Police (FATA) is actively working to identify the breach’s source.

However, the company maintains that customers’ payment data, especially card security codes (CCV), passwords, and expiration dates, remain secure and were not accessed by hackers.

Agreement between Snappfood and “irleaks”?

In a subsequent tweet on January 1, 2024, Snappfood claimed that an agreement had been reached with the hacker group, preventing the sale or leakage of the data online. While the specifics of the agreement remain undisclosed, Snappfood’s claim appears substantial, given that the hacker group had deleted their post from Breach Forums and removed the sample link previously shared on the forum and their Telegram channel at the time of writing.

Additionally, a post from the hackers on their Telegram channel confirms the agreement and outlines the next steps for the affected company and customers. The following content has been translated using Google Translate:

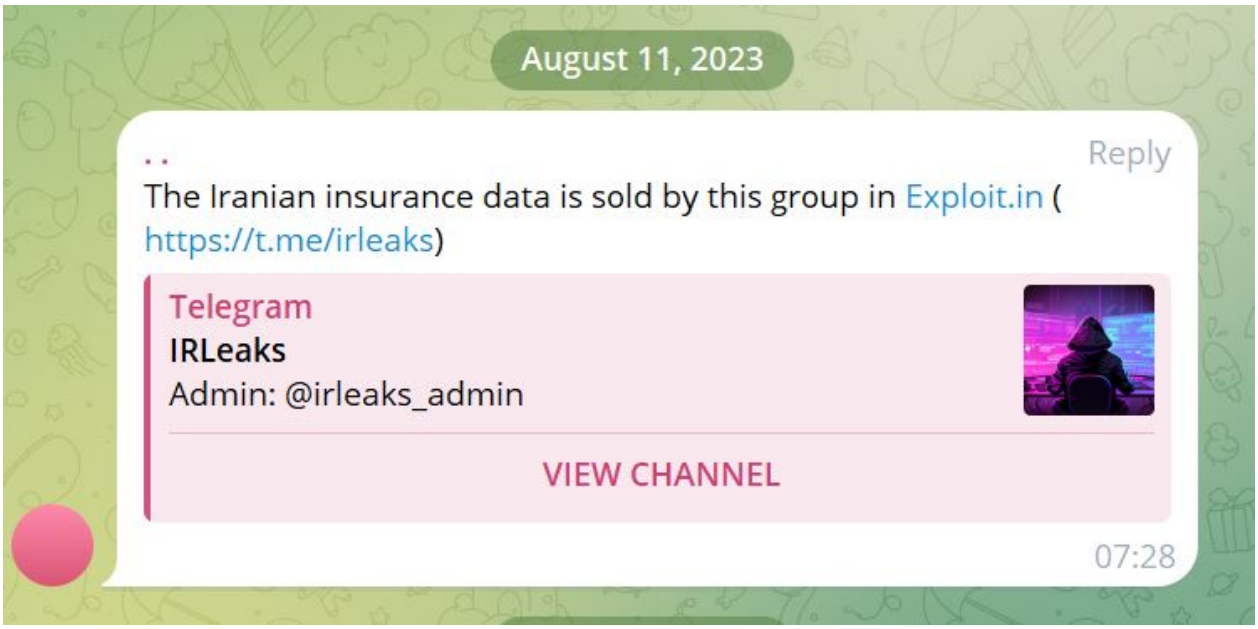
> *The issue of Sold Out in one of the forums was that due to the uncertainty of the negotiation outcome for our team, we decided to temporarily write “sold”; But now after getting confirmation from Snapfood, we deleted the post completely.*
>
> *Following the negotiations we had with the Snapfood team, the data of this collection has not and will not be sold to anyone. Snapfood’s management team showed that people’s information and brand reputation are more valuable to them than anything else.*
>
> *irleaks*

Telegram post by irleaks confirming the agreement – Screenshot credit: Hackread.com

Nevertheless, if both parties adhere to their agreement, it could be deemed a positive outcome for the company and its customers. Hackread.com has reached out to the hackers for a potential interview about the data breach, and this article will be updated accordingly if they respond.

Who is “irleaks”?

The identity of “irleaks” remains unknown, but the group is known for communicating in the Persian language. This is the same group that, in August 2023, was selling insurance data of Iranian citizens on the well-known private Russian hacker forum Exploit.in.



Screenshot credit: Hackread.com

Iran and Cyber Attacks

This incident is not the first instance of a high-profile company like Snappfood falling victim to a data breach. **In April 2019**, TAP30 (now TAPSI) exposed its database, revealing the personal details of millions of drivers and customers. Additionally, **in May 2021**, the Raychat app, a popular Iranian social and business messaging platform, was hacked, resulting in the leakage of data from more than 150 million users.

RELATED ARTICLES

1. Personal details of 42M Iranians sold on a hacking forum
2. Disruptions at 70% of Iran's Gas Stations Blamed on Cyberattack
3. Anonymous Hits Iranian State Sites, Hacks Over 300 CCTV Cameras
4. Iran State-Run TV's Live Transmission Hacked by Edalate Ali Hackers
5. Iranian State TV Hacked During President's Speech on Revolution Day