Pilfered Data From Iranian Insurance and Food Delivery Firms Leaked Online

oodaloop.com/briefs/2024/01/04/pilfered-data-from-iranian-insurance-and-food-delivery-firms-leaked-online/

OODA Analyst January 4, 2024

Cybercriminals broke into the systems of 23 Iranian insurance firms and SnappFood, an online food ordering service and dumped millions of user profiles. The sample from the insurers' leak include names, phones, identity numbers, addresses, passport numbers and other sensitive details. The insurance firms include Kowsar, Atieh, Asia and Albert. The data appears to be genuine, according to security researchers as Hudson Rock.

After the attack on the insurance firms, the attackers "irleaks" bragged about breaking into the system of SnappFood. The attackers claimed to have exfiltrated 3TB of highly sensitive data. The data allegedly is from 20 million user profiles, including emails, passwords, phone numbers. The data also includes 51 million users' addresses and 600,000 credit card records. SnappFood issued a statement that it was working with local agencies to identify and remove the source of pollution caused by the hacking group. Hudson Rock identified that a computer used by a SnappFood employee was infected with the StealC info-stealer. This is not the confirmed source the attack, but the malware created a conduit through which sensitive data could have been extracted.

Read More: Pilfered Data From Iranian Insurance and Food Delivery Firms Leaked Online