Cyber ✶ Chaos

Volume 2

By: Dr Malvika Mehta

The alleged ‘Aadhar data of 815M+ Indian citizens leak, 2023’

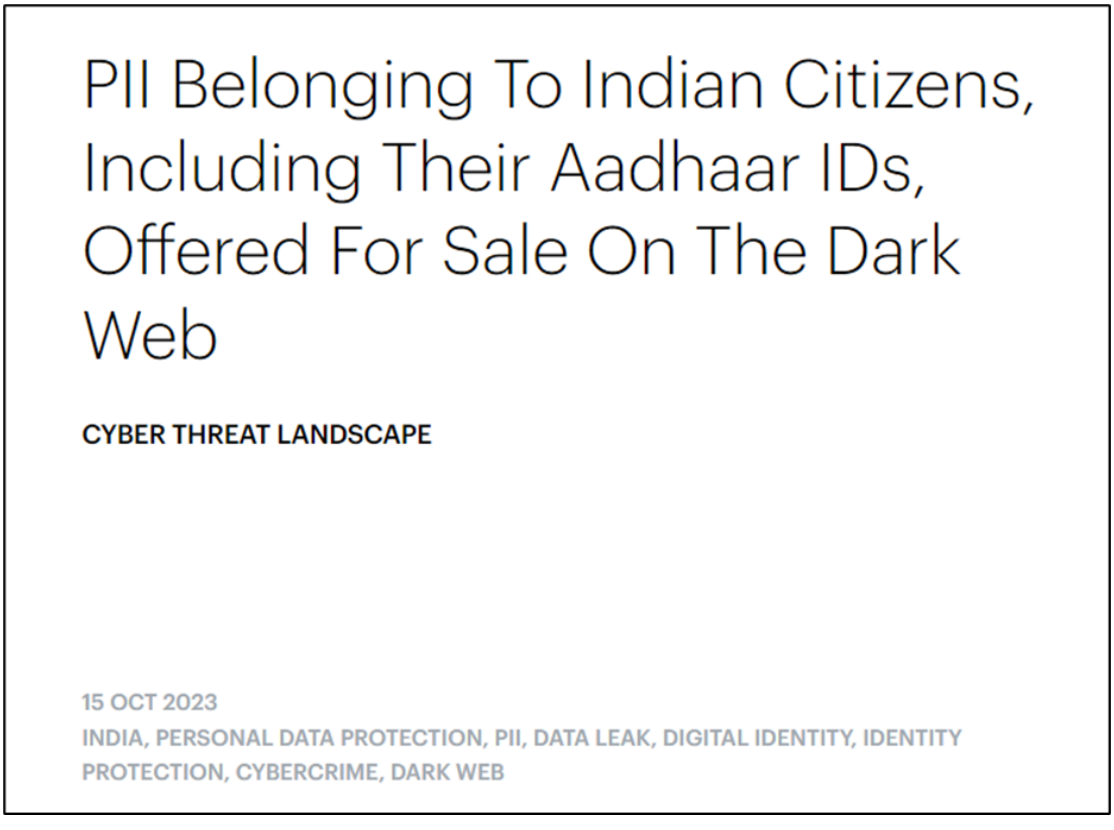
“Aadhar data of 815 M+ Indian citizens leak, 2023”

INTELLIGENCE & INVESTIGATIONS | By: Dr Malvika Mehta | DATE: 02/11/2023

*The findings in this report are solely based on individual research done using open source investigations. There may be future developments as information continues to unfold and new evidences come into picture.

India’s biggest leaked database on the underground forum

Resecurity is a cyber security company based out of California, they had reported a data set on sale (9th October 2023) containing crucial and sensitive information such as Aadhar and passport details of Indian citizens on the darknet.


PII Belonging To Indian Citizens, Including Their Aadhaar IDs, Offered For Sale On The Dark Web

CYBER THREAT LANDSCAPE

15 OCT 2023

INDIA, PERSONAL DATA PROTECTION, PII, DATA LEAK, DIGITAL IDENTITY, IDENTITY PROTECTION, CYBERCRIME, DARK WEB

Figure 1 Blog posted by Resecurity, a US based cybersecurity firm mentioning about the Indian database on sale in the darknet.

Database information

Date Of leak: 2023-09
Country Of leak: India
Number Of Data: 815M+ unique
Size: 90GB
Format Type: ZIP-CSV
Accept middleman

Figure 2 Database properties.

Claims were made by several news channels that the data was reportedly stolen from a database belonging to the Indian Council of Medical Research (ICMR) and/ or UIDAI.

However, no connection has been established yet with ICMR database, or covid- 19 or health related PII based on OSINT investigations. Prima facie, the claims appear to lack credibility or seem fake.

This is not the first time that Aadhaar database has leaked and is up for sale in underground forums. There have been several data breaches involving Aadhaar data in the past. There are similar files found on the darknet forums, dating back in time.

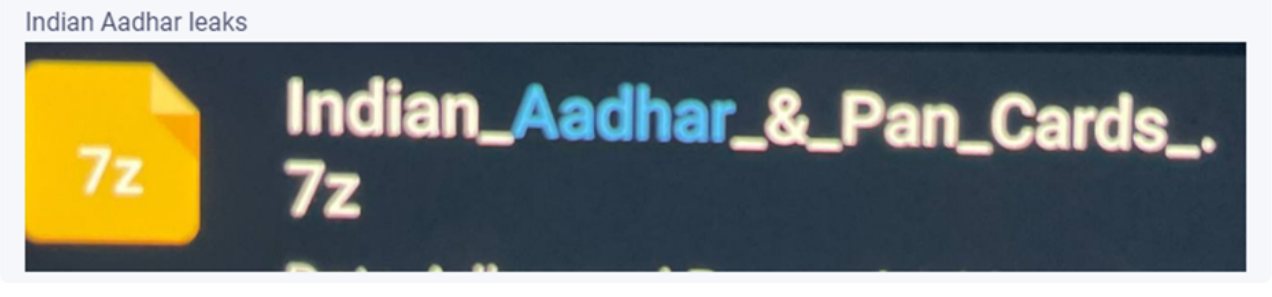


Figure 3 Leaked files containing Indian data.

Such data being easily available on accessible forums of the internet raises serious concerns about the security of Aadhaar and passport data. Aadhaar is a unique identification number that is issued to all Indian citizens, and it is used for a wide range of purposes, including accessing government services and financial accounts.

Threat actor

Pwn001

The threat actor is Pwn001 who released sample data sets and claims to have 815M+ unique PII of Indian citizens.

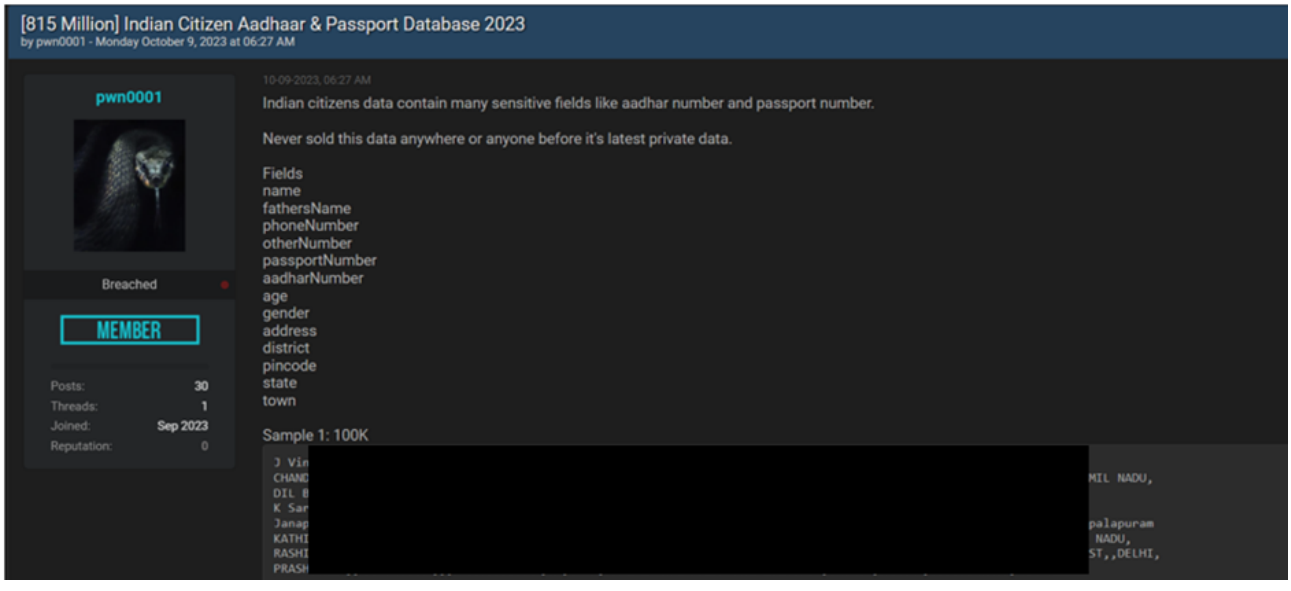


Figure 4 Pwn0001's post on a darknet forum.

The user had first posted a thread on Breach forums on 10th October 2023 mentioning that the database will be sold to only one person. Sample files were uploaded in the thread following the post.

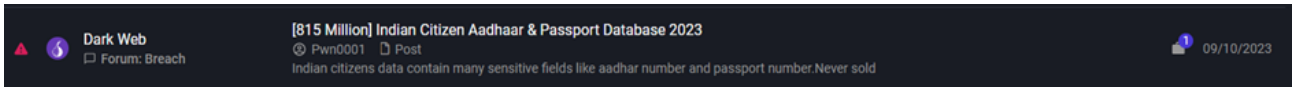


Figure 5 Pwn0001 mentioning about the availability of 815M+ unique datasets.

Figure 6 Continued thread from pwn0001's post.

On 18th October 2023, pwn001 mentioned that the leaked database is not from UIDAI database but from a different government source. It includes a good number of Aadhar and passport documents.

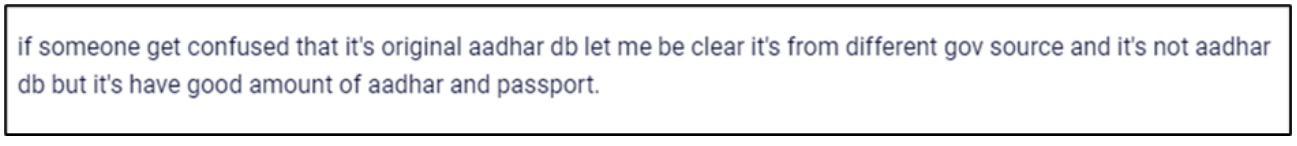


Figure 7 It is not the original AADHAR database.

The comments from other users on this thread does highlight the demand for databases like these.

User pwn001 was online on 31st October 2023 for 12 seconds on one of the darknet marketplaces. The account is fresh, created on the same day- account not activated.

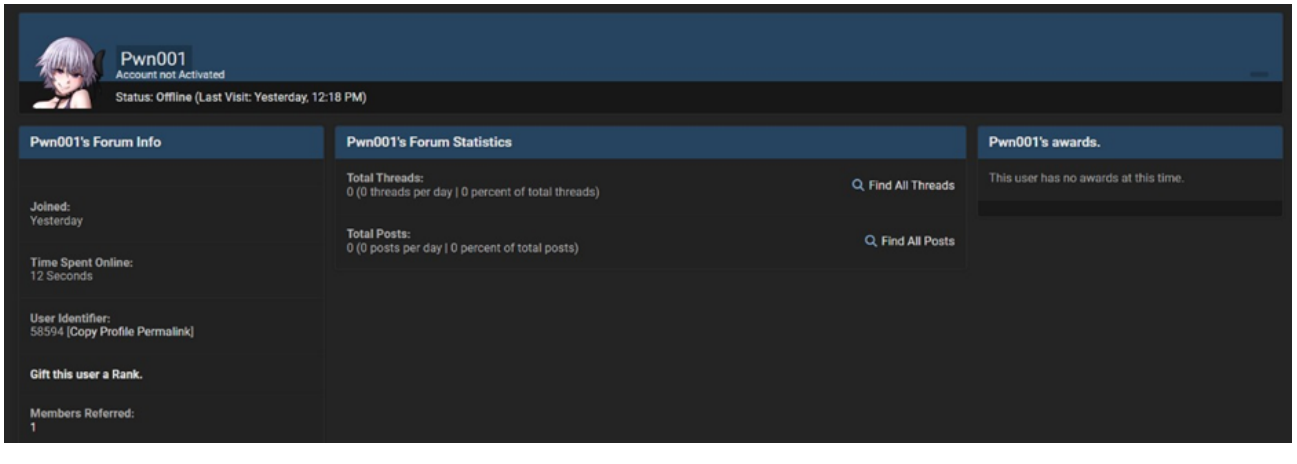


Figure 8 Another user account- Pwn001 not activated on the darknet forum.

User pwn0001 joined the forum on 28th September 2023 and the account is active on the forum. However, no posts or threads were found.

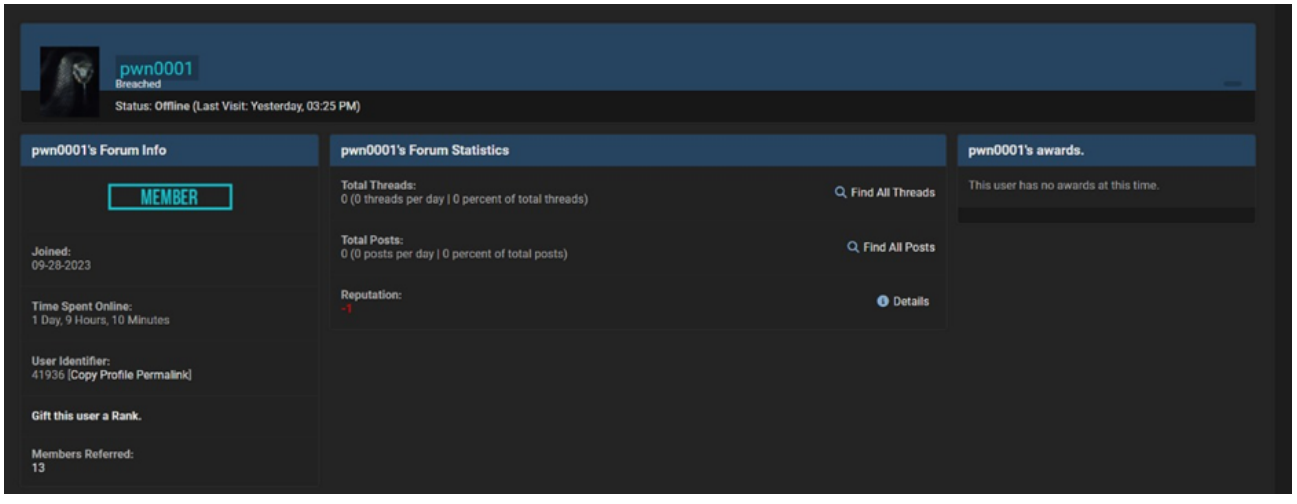


Figure 9 @Pwn0001, existing user on the darknet forum.

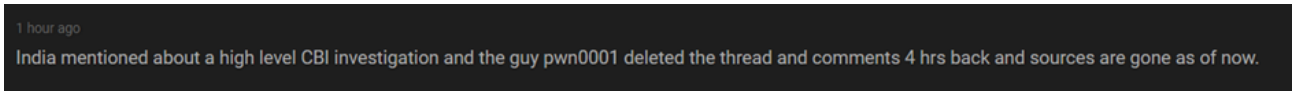


Figure 10 Deleted thread ever since the information about the leak has been on the news.

Sample data analysis

Contents of the sample file

This type of data is commonly stored by mobile network operators, and it is crucial for providing mobile services and complying with various legal and regulatory requirements.

MSISDN, Name, Date of birth, Father Name, Local Address, Permanent Address, Alternate No, Email Id, Gender, Nationality, Connection Type, SIM Activation Date, Aadhar, Photo Id Proof Details, Address Proof Details

Sample data has been verified; data is accurate and valid.

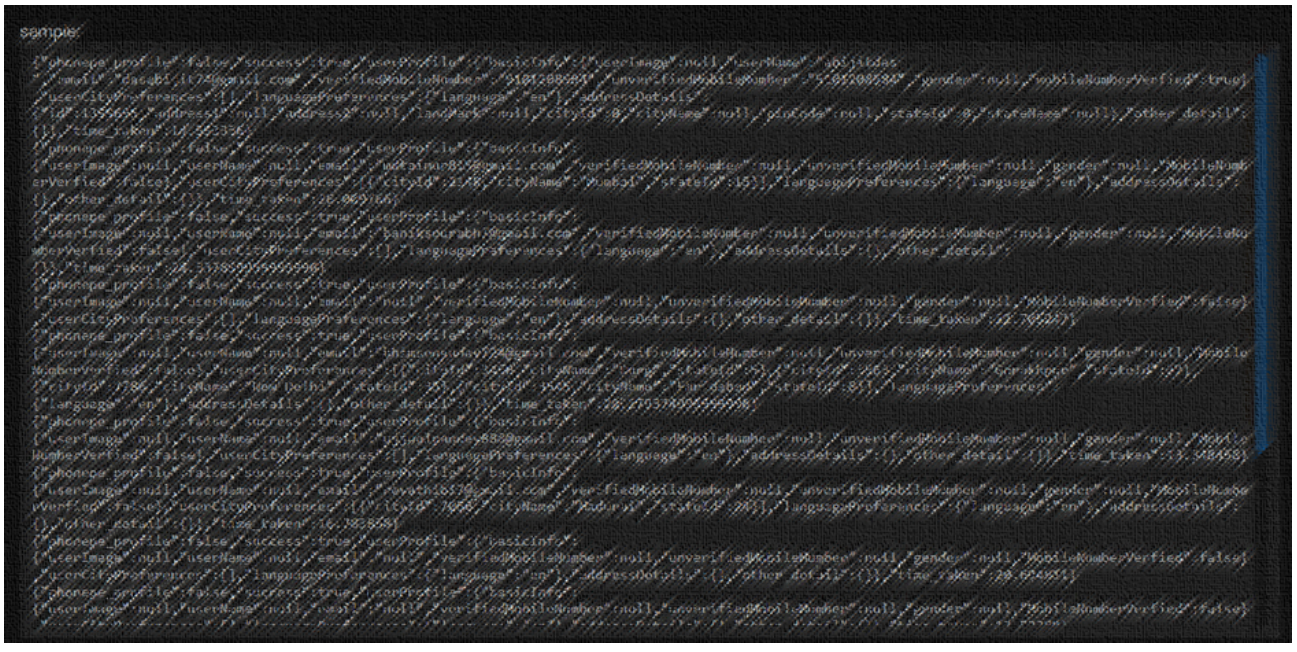


Figure 11 Sample data masked considering privacy.

Based on the files that were found, it is likely that the breached database is related to the telecommunications industry or mobile service providers. The presence of MSISDN (mobile phone numbers), SIM Activation Date, and other mobile-related information strongly suggests this.

Additionally, the inclusion of Aadhar (an identification number used in India) and Photo ID Proof Details and Address Proof Details may indicate that the data pertains to customers in India or regions where such documentation is required as proof for obtaining mobile services.

The phone numbers belong to prepaid- Airtel users (from the 226 rows of sample data set).

While there were many other sample files released, at the time of this research they were removed from the forums. It may be a possibility that this is one type of a file from the entire leak, there may be chances of other Indian databases fused in to achieve 815M+ target.

Other leaked data on the darknet (Indian databases)

Prior to this data breach, on 23rd September 2023, 2022, and 2021 a similar database made its way to the darknet market. However, the link no longer exists.

Darkleakmarket	True Caller Indian Data Leak	2021-09-09
Darkleakmarket	Indian Aadhar data & software.	2021-10-07

Group	Title	Date
Darkleakmarket	Indian Aadhar data & software.	2021-10-07

Channel	Message	Date
Meganzshare	印度银行POS刷卡机数据（含有卡号，身份证等数据） Indian Bank POS card reader data (including card number, ID card, etc.) Contact: @Crazysnows ----------reg_id 注册idappgenlet appgenletIDapp_fullname 全民father_name 父亲的名字mother_name 母亲的名字gender 性别dob 生日country_code 国家代码moblie_no 手机号码email 电子邮件bank_name 银行名称branch_name 分支机构名称pos_code pos代码aadhar_no ad身份证号码pan_no Pan身份证号码address1 地址1address2 地址2address3 地址3state 州市district 区pincode pincodehigh_edu_qua 学历year_of_passing 年份possignupfor possignupforsyllabus 教学大纲acc_holder_name acc持有人姓名account_no 银行卡帐户号码ifsc_code ifsc代码mode 模式emp_code emp代码area 区域region 地区data 数据----------	2022-10-22T03:45:59+00:00

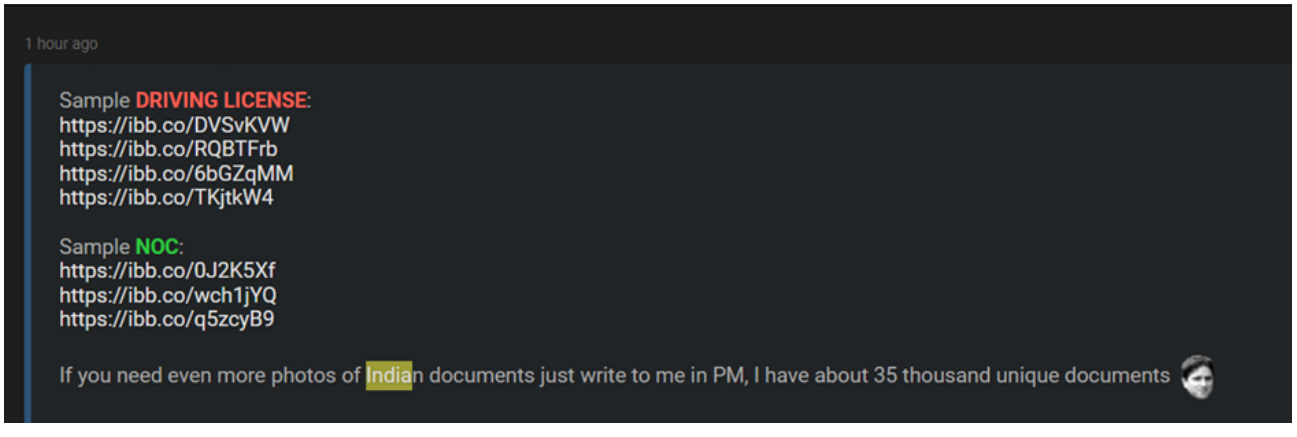


Figure 12 Other leaked databases containing PII of Indian citizens.

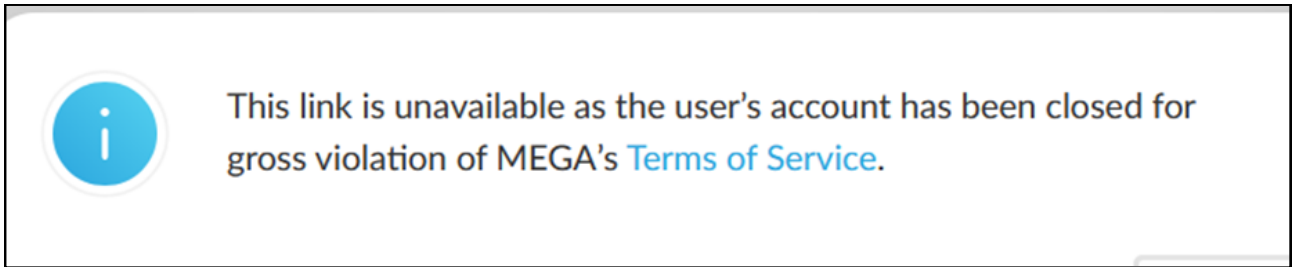
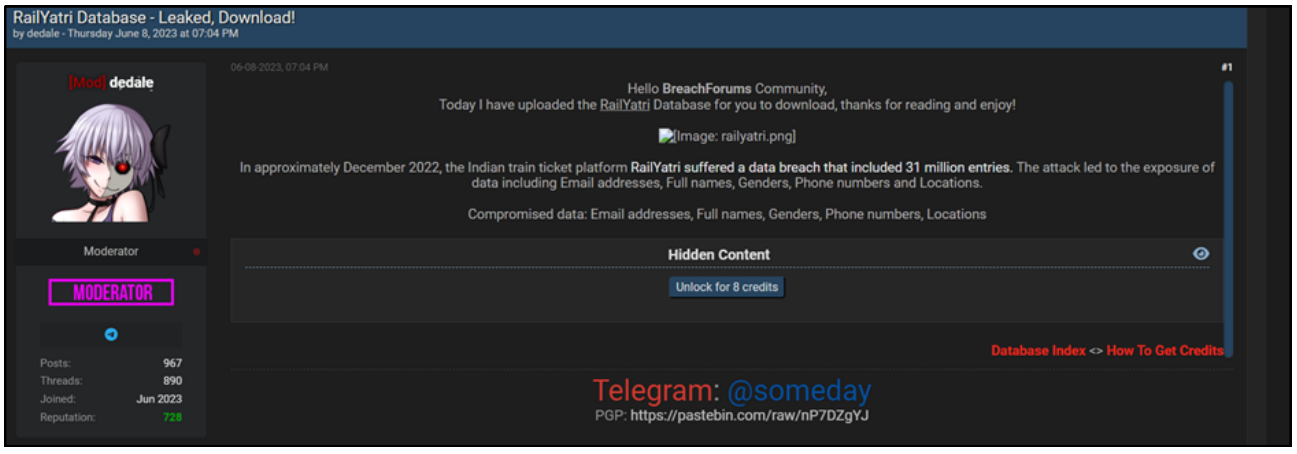


Figure 13 Sample data files have been removed from cloud service providers like Mega.

In June 2023, Rail Yatri database was found on the same forum.



In 2021, Covid-19 vaccination database containing information about 150 million vaccinated people of India was sold at 800 USD.

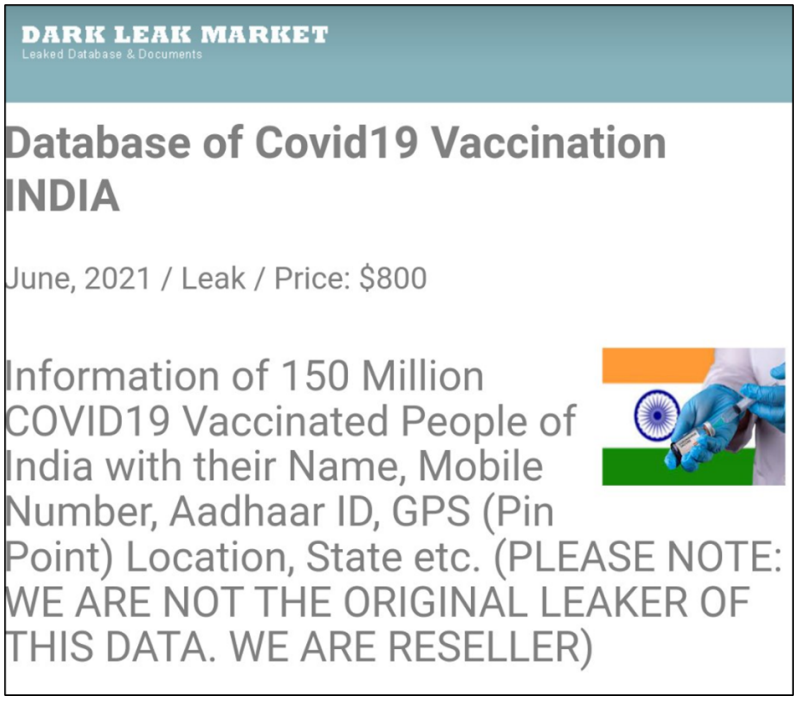


Figure 14 2021 Covid-19 vaccinated people's database sold on the darknet markets.

Hackers claim to have leaked Indian databases containing sensitive information like full name, DOB, address, identity numbers, financial information on channels of Telegram.

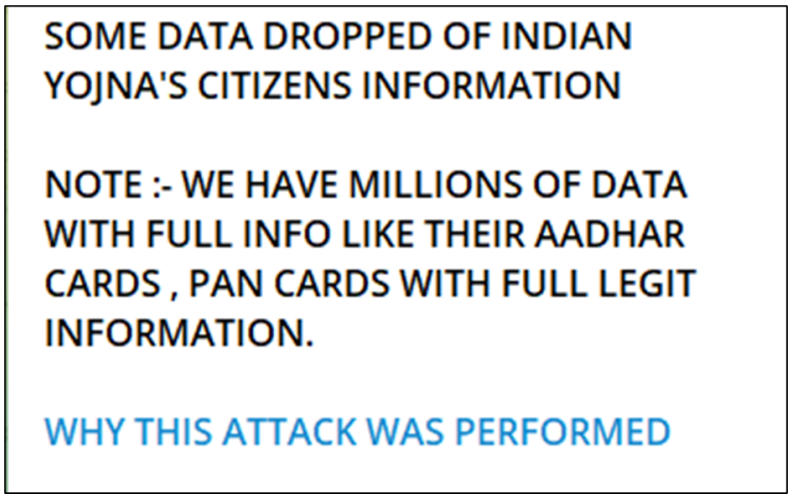


Figure 15 Message on Telegram in September 2023.

Some channels on Telegram have been providing sensitive information of Aadhar and Pan card to buyers:

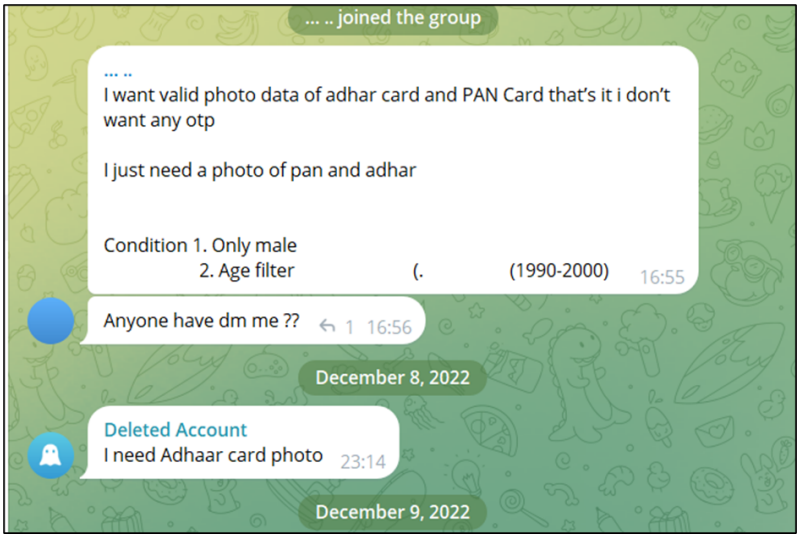


Figure 16 Sensitive data sold on Telegram channels- Aadhar and PAN card details.

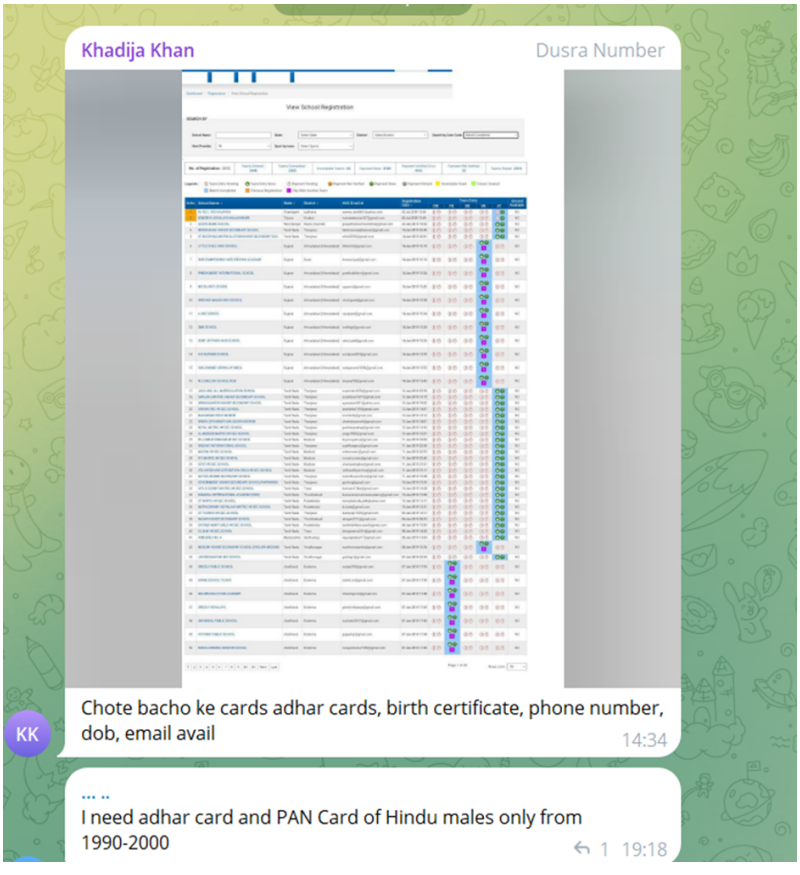


Figure 17 Service providers selling Indian identity cards, certificates and PII on Telegram.

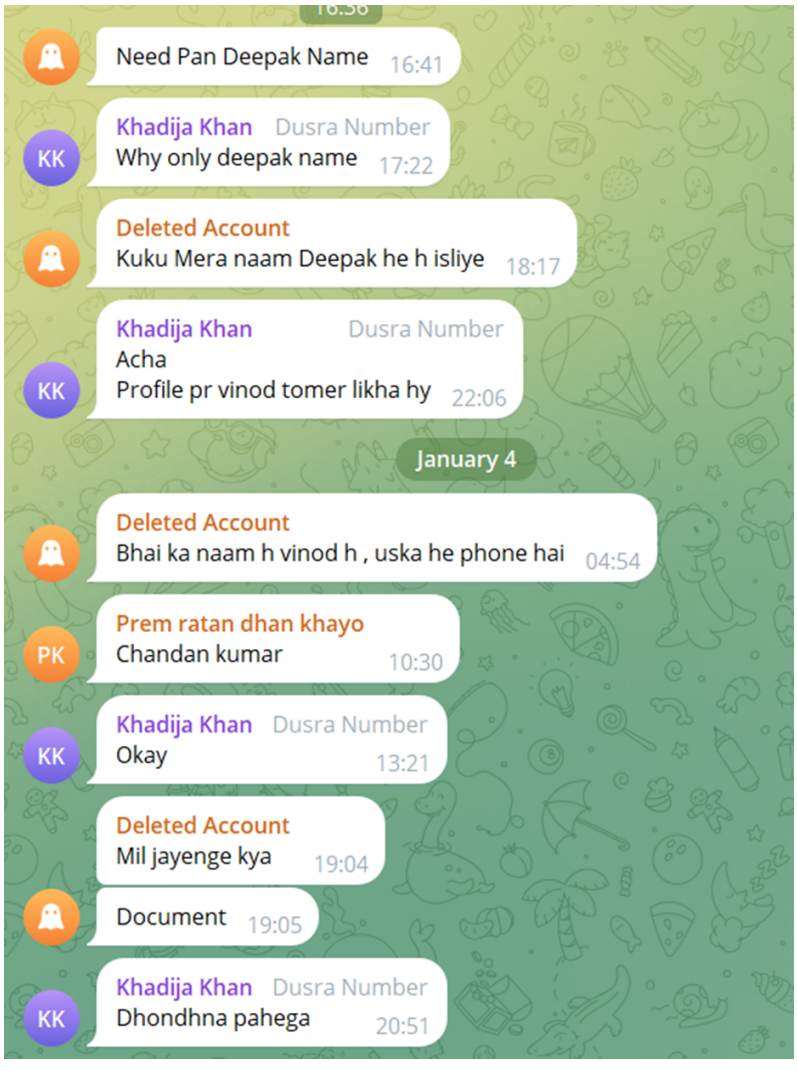


Figure 18 Service providers selling Indian identity cards, certificates and PII on Telegram.

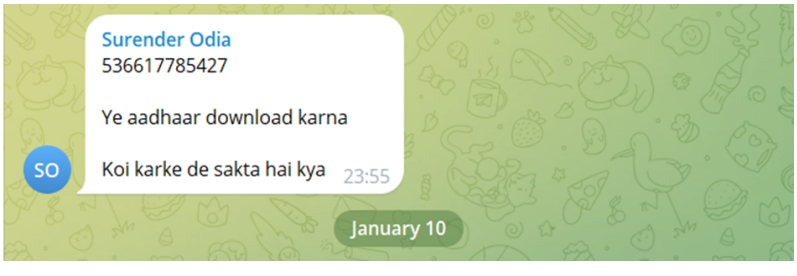


Figure 19 Service providers selling Indian identity cards, certificates and PII on Telegram.

These Aadhar cards were used with the intention of linking sim cards/ mobile numbers and WhatsApp accounts. The threads have several users asking for delivery of fake sim cards.

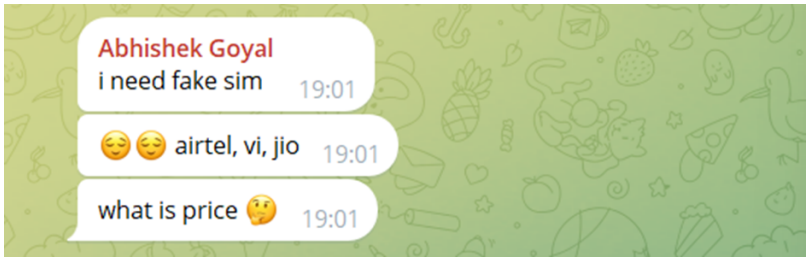


Figure 20 Fake sim requirements on Telegram.

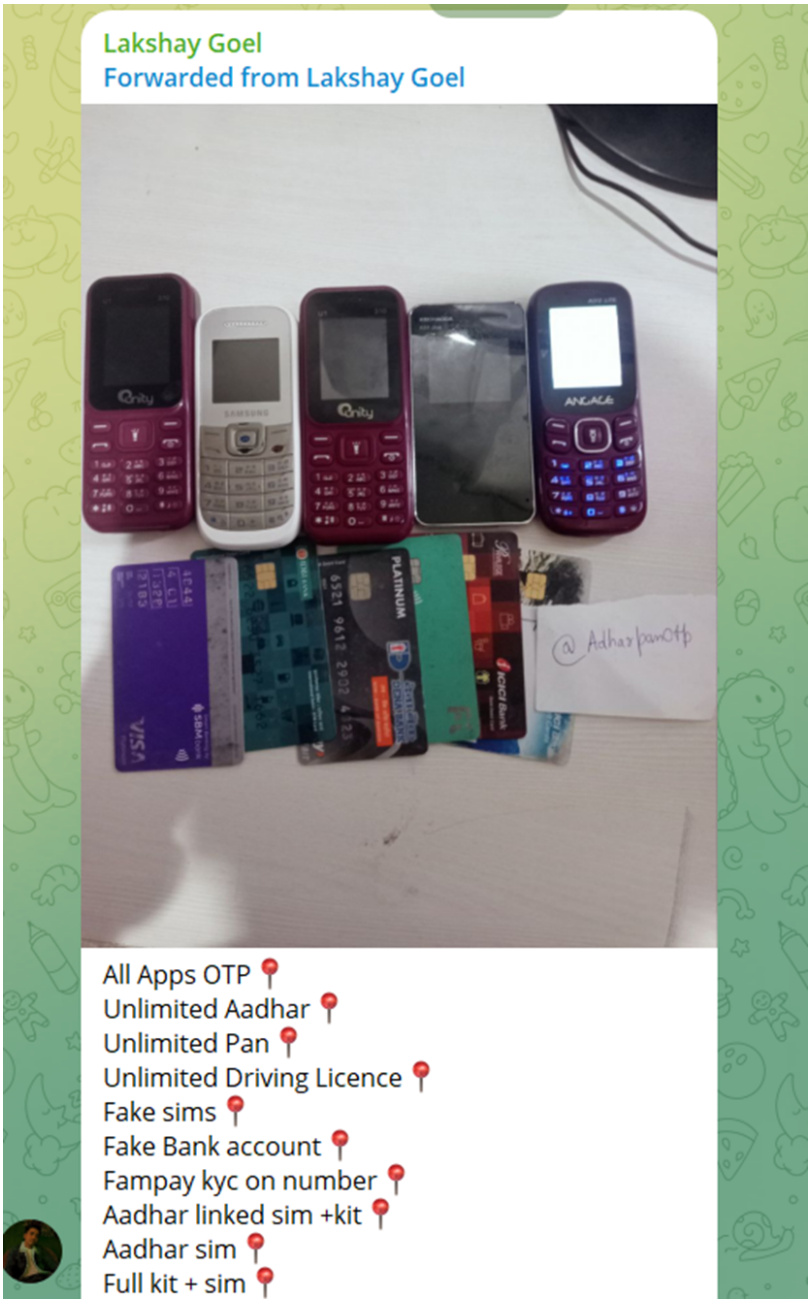


Figure 21 Fake bank accounts, Aadhar linked sim kits, driving licences, PAN cards sold on Telegram.

In February 2023, a channel on Telegram posted Pan card numbers.

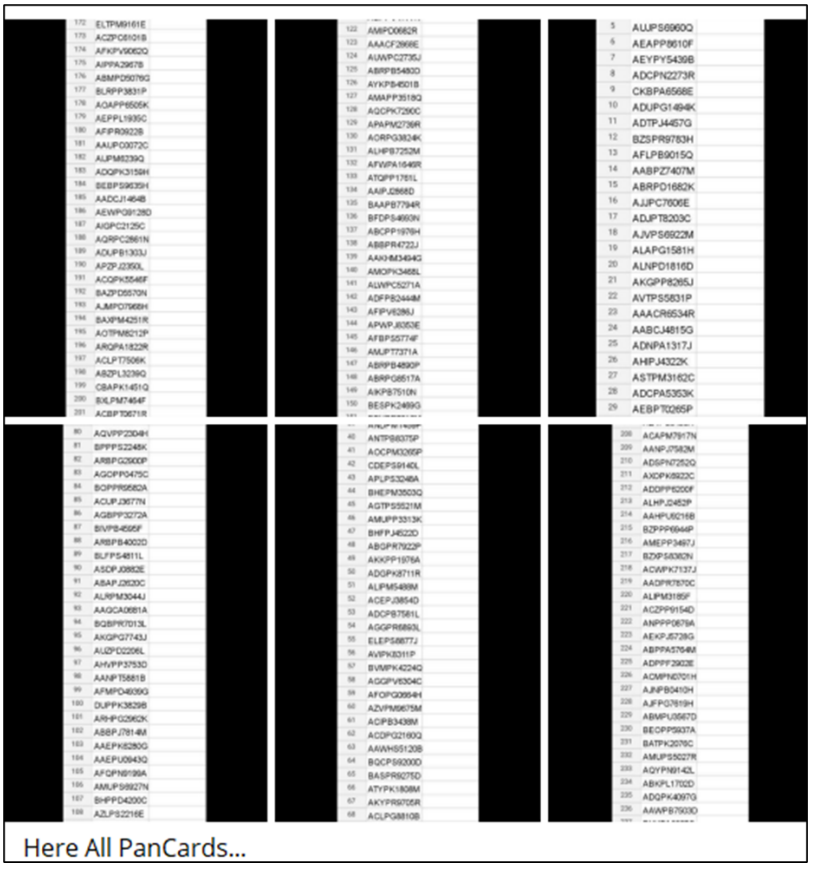


Figure 22 List of PAN numbers being circulated freely.

Databases of tax defaulters were also released in September 2023.

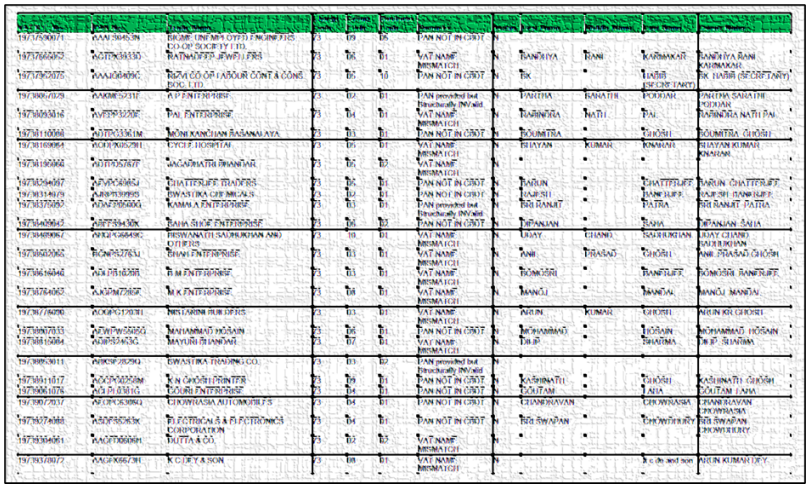


Figure 23 Leaked database of tax defaulters, masked for privacy.

Figure 24 Indian identity cards data sold on Telegram channels.

Similarly, several other data leaks of third-party service providers have suffered from massive data breaches like that of Air India.

After the latest activity from @pwn0001, there were many other databases that were uploaded on the darknet markets as an opportunity by the hackers.

Potential misuse?

Identity theft, criminals can use stolen PII to create fake identities, which they can then use to commit crimes such as fraud, theft, and money laundering.

Financial fraud, criminals can use stolen PII to access victims' bank accounts and credit cards, or to apply for loans and other financial services in their names.

These databases are also used to trick and earn money using mobile numbers, email ID's. This channel on YouTube trains people to create multiple accounts and register using several credentials (that do not belong to the individual) to earn cashback and rewards.

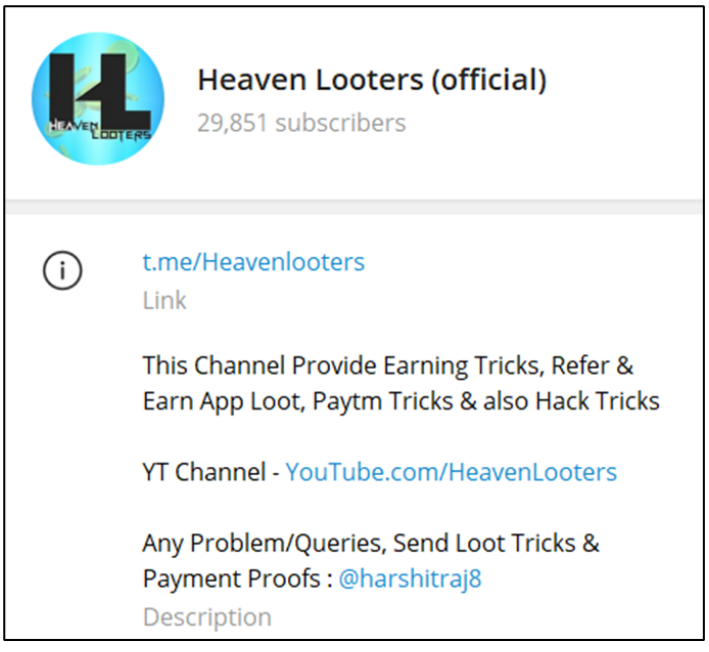


Figure 25 Examples of potential misuse of breached & leaked databases.

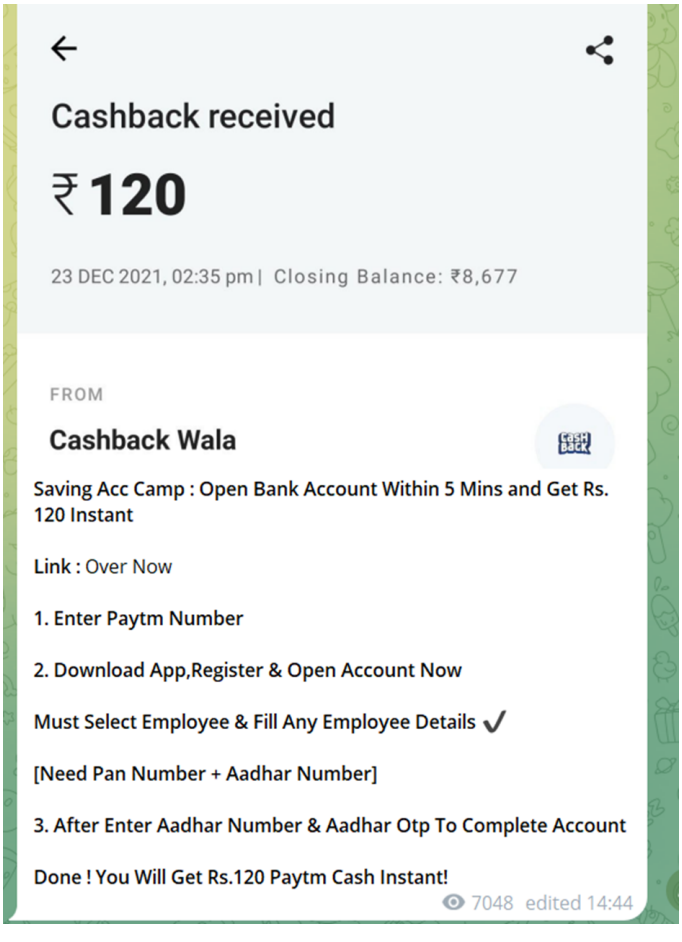


Figure 26 Examples of potential misuse of breached & leaked databases.

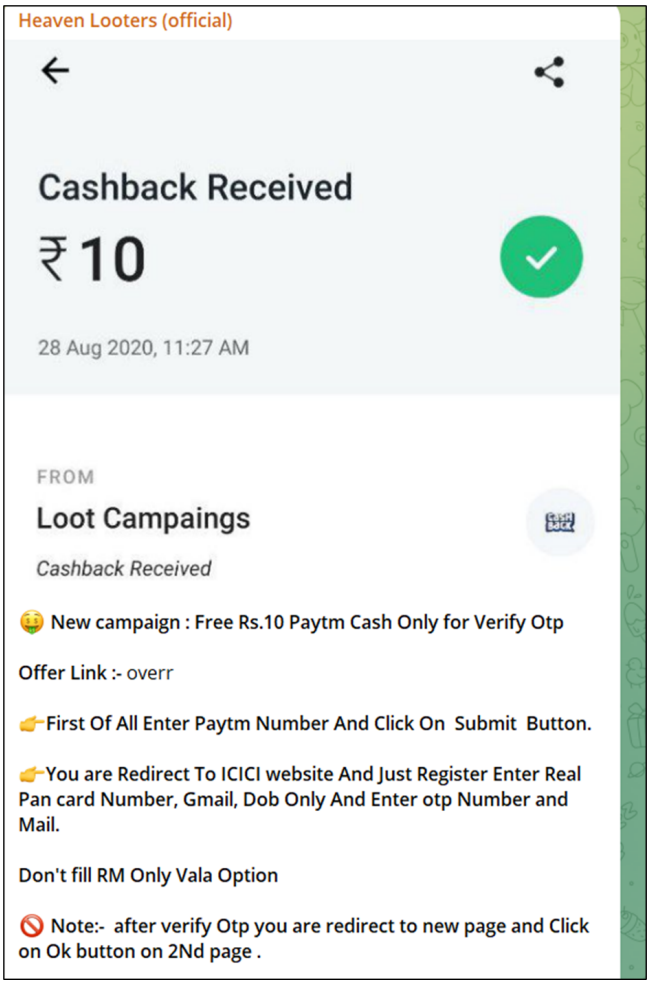


Figure 27 Examples of potential misuse of breached & leaked databases.

Current developments & recommendations

While the investigations are still on, the government had already taken steps to improve the security of Aadhaar data, such as introducing a voluntary locking system for Aadhaar biometrics.

Regardless, there needs to be more to increase the security of such databases such as restricting its usage. Regular monitoring of assets like these across the internet is required, adoption of latest technologies to assist human intelligence is the need.

Cyber threat intelligence is a growing domain and thus the demand for specifically skilled individuals is on the rise. News & media forums must validate all the claims before making statements, it has become even more crucial to tackle misinformation and disinformation in this digital world.

Additionally, the government must take steps on:

- **Implementing a zero-trust security architecture**. This would involve verifying the identity of all users and devices before granting access to resources, regardless of whether the user or device is inside or outside the government network.

- **Adopting a risk-based approach to cybersecurity**. This would involve identifying and prioritizing the government's most critical assets and vulnerabilities and implementing security controls accordingly.
- **Investing in cybersecurity training and awareness for government employees**. This would help to reduce the risk of human error, which is a leading cause of data breaches.
- **Partnering with the private sector to share information and expertise on cybersecurity threats.** This would help the government to stay ahead of the curve and better protect its critical infrastructure.
- **Develop a national cyber threat intelligence program.** This would involve collecting and analysing information about cyber threats from a variety of sources and using this information to develop and implement security measures to protect critical infrastructure.

The government should also **invest in developing and adopting new cybersecurity technologies, such as artificial intelligence (AI) and machine learning (ML).** AI and ML can be used to detect and prevent cyber threats more effectively than traditional security solutions.