

The logo for FLASH, featuring a white globe icon with a lightning bolt symbol inside, followed by the text "FLASH" in large, bold, white capital letters.

FLASH

Alleged Data Breach by ChinaDan

ZEROFOX INTELLIGENCE

F-2022-07-06a

Classification: TLP White

Criticality: High

Intelligence Requirements: PII & Fraud, Deep Dark Web & Criminal
Underground

July 6, 2022



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 July 6, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

Alleged Data Breach by ChinaDan

Key Findings

- On June 30, 2022, a threat actor advertised 23 terabytes of personally identifiable information (PII) from the Shanghai National Police for sale. The data is priced at 10 BTC (approximately USD 200,000).
- The database allegedly contains the PII of one billion Chinese victims' names, addresses, birthplaces, national ID numbers, telephone numbers, and criminal history.
- At the time of writing, it is unclear how the threat actor obtained the database being advertised.

Analyst Commentary

On June 30, 2022, new but positively-trending threat actor “ChinaDan” advertised a database that allegedly contains 23 terabytes (TB) of PII from the Shanghai National Police on the Deep Web English language forum breached[.]to (see Figure 1 below). The threat actor shared a sample of 750,000 records, which were comprised of three JSON files containing victims’:

- Names
- Addresses
- Birthplaces
- National ID numbers
- Telephone numbers
- Criminal background information

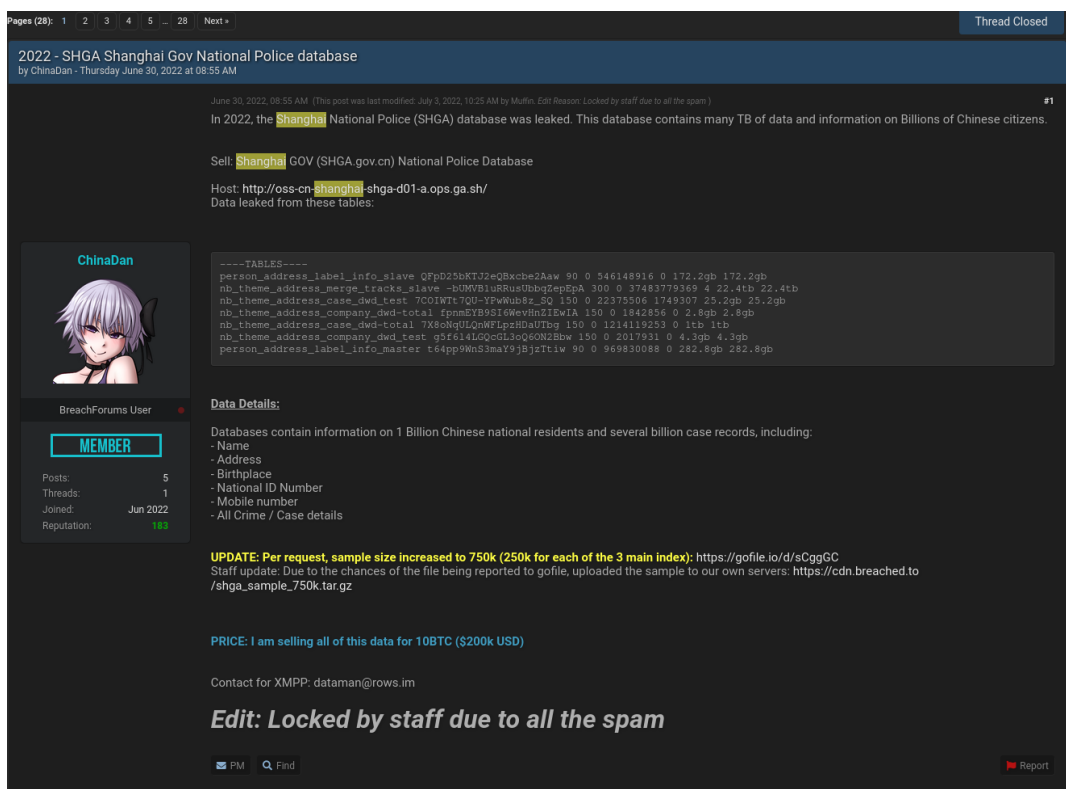


Figure 1: ChinaDan's original post on Breached[.]to

Source: ZeroFox Intelligence

ZeroFox Intelligence acquired the following sample files shared by the threat actor as evidence of the breach:

- “address_merge_with_mobile_data.json” – 151 MB
- “case_data_index.json” – 321 MB
- “person_info.json” – 114 MB (see Figure 2 below)

Obtaining these sample files allowed ZeroFox to confirm the data exists; while the samples do not verify ChinaDan's claims in their entirety, they do lend more credibility to the forum post than just the advertisement alone. In addition, the file samples' names and screenshots offer unique data points not covered by most mainstream media. Further, the .json files acquired from ChinaDan can be searched for specific datasets.



```
{ "_id": " ", "_index": "person_address_label_info_master", "_score": null, "_source": { "AGE": -
, "BIRTHDAY": " ", "BPLACE": " ", "EDEGREE": " ", "ESCU": " ";
, "HEIGHT": " ", "HHPLACE": "
", "IDNO": " ", "IDTYPE": " ", "LABELNAMES": " ", "LABS": "
", "MARR": " ", "NATION": " ", "NPLACE": " ", "PHOTO": "{
shga-d01-a.ops.ga.sh/shga-ryzp/CRJ/CRJ_APPLY_PHOTO/
shanghai-shga-d01-a.ops.ga.sh/shga-ryzp/SYRK/SYRK_T_ZP_EDZ/
shanghai-shga-d01-a.ops.ga.sh/shga-ryzp/JJLHY/JJLHY_DRV_PHOTO/-
DRV_PHOTO_
PHOTO/PHOTO_XP_GNBZ/XP_GNBZ_
} }", "PROF": "职员", "QUERY_STRING": "
", "RELI": " ", "RNAME": " ", "SEX": " ", "STD_ADDRESS": "
", "_type": "a", "sort": [ ] }
```

Figure 2: Sample data shared by the threat actor. File: “person_info.json” (~250,000 records)

Source: ZeroFox Intelligence

The threat actor claimed approximately one billion Chinese residents are impacted by this breach, which comprises several billion case records. The threat actor priced the database at 10 BTC (about USD 200,000). No further details were disclosed publicly in this post, including how the threat actor procured the database. ZeroFox researchers note that this advertisement is the only activity ChinaDan has on the forum at this time, making the reputation of the threat actor difficult to confirm.

Recommendations

- Due to the highly-sensitive nature of the PII contained in this database, ZeroFox assesses that it is highly likely that victims will be at risk of identity theft and other forms of fraud. It is advisable to exercise additional caution and enforce stricter know-your-customer (KYC) verifications during new account creation or account recovery of Chinese nationals.
- Organizations should be aware that employees from China are at an increased risk of being targeted because of this breach.
- Utilize account permissions best practices, such as role-based access control, least privilege, and restricting root/admin permissions.
- Segment critical network resources using zero-trust configurations.
- Enforce best practices on passwords, such as complexity, forced expiration, and prohibiting password reuse.
- Do not share passwords, and do not reuse the same password on different websites and applications.
- Log and monitor all administrative actions as much as possible. Alert on any suspicious activity.
- If you are alerted or suspect a compromised account, change the password immediately.



Appendix: Traffic-Light Protocol for Information Dissemination

Red

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.

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.

Amber

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.

Recipients may ONLY share TLP:

AMBER information with members of their own organization and only as widely as necessary to act on that information.

Green

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.

HOW MAY IT BE SHARED?

Recipients may share TLP:

GREEN information with peers & partner organizations within their sector or community but not via publicly accessible channels.

White

Sources may use TLP:

WHITE when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

TLP:

WHITE information may be distributed without restriction, subject to copyright controls.