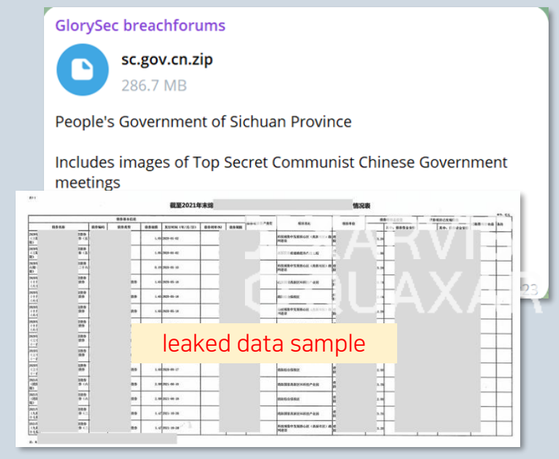
Dark web & Telegram Weekly Highlights

August Week 4

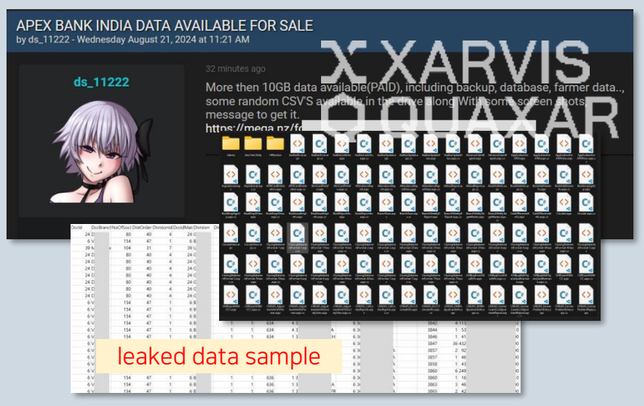
Internal Documents of Chinese Local Government Leaked. Currently Available for Free on a Dark Web Hacking Forum

- A post sharing files leaked from a government agency in Sichuan, China, has been published on the dark web hacking forum, BreachForums.
- On August 20, a forum threat actor named "ronioum" posted that they were releasing data from a government agency in the Sichuan region for free. According to the post, the data is approximately 2GB in size and contains about 2 million lines of information.
- Upon checking the data through the Telegram address provided by the threat actor, it was confirmed that the data includes various types of information such as log data, various photos and images, and SQL data.
- In addition to this data, other Chinese-related data and data from Pakistan were also found on the Telegram channel.



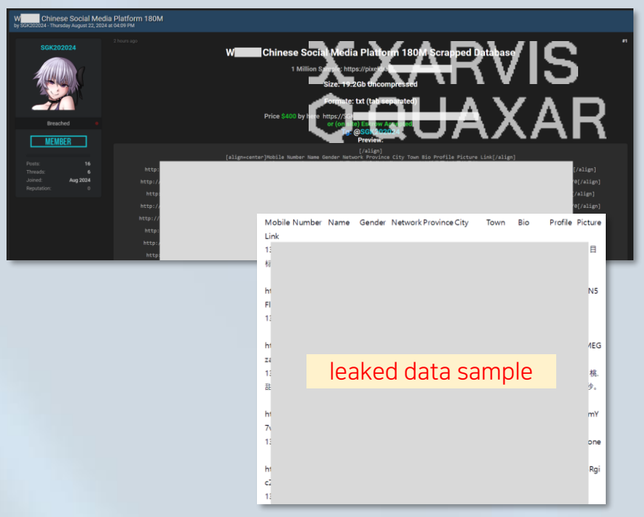
Leak of internal data from an Indian bank detected, including suspected customer information and transaction histories

- Internal documents from India's commercial bank "A Bank" have been leaked and are being sold on the BreachForums hacking forum.
- On August 21, a forum threat actor named "ds_11222" posted that they were selling data from "A Bank." The leaked data is approximately 10GB in size, and the threat actor provided a sample of the leaked data through a separate link.
- Reviewing the link revealed three image files with screenshots of leaked data lists and five Excel files with suspected customer information and transaction history.



Internal data of China's popular messenger W*** leaked and sold, including sensitive information like profile photos

- Internal data from the global messenger W****, owned by the well-known Chinese company Tencent, has been leaked and is being sold on BreachForums.
- According to the seller, SGK202024, the data consists of approximately 19GB of TXT files. The leaked content includes a wide range of sensitive information, from basic details like threat actors' names, genders, and residences, to more sensitive data such as mobile numbers, bio profiles, and photos.



- The seller released a sample of the data in the post and also provided a link to download a file approximately 200MB in size. Upon reviewing the data, it was found to contain over 30,000 pages of extensive information.

S2W

About S2W

- S2W is a big data intelligence company specialized in analyzing hidden channels and cryptocurrencies.
- S2W captures massive amount of data from various channels and conducts analysis with the unique AI based multi-domain analytics engine.
- S2W offers a threat intelligence solution S2-XARVIS,
- Detection of brand abuse site, phishing site, real-time threat monitoring solution QUAXAR,
- Cryptocurrency anti-money laundering solution S2-EYEZ,
- Digital fraud detection system S2-TRUZ.

Contact

For any queries, please contact support@s2w.inc / www.s2w.inc