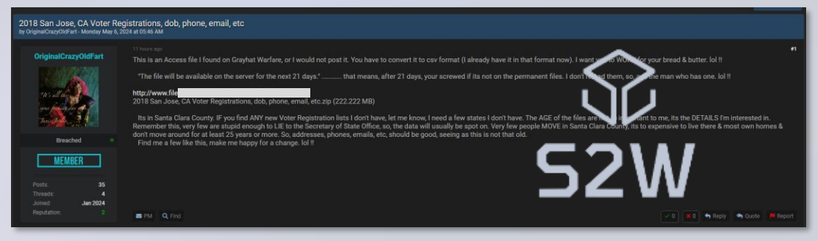
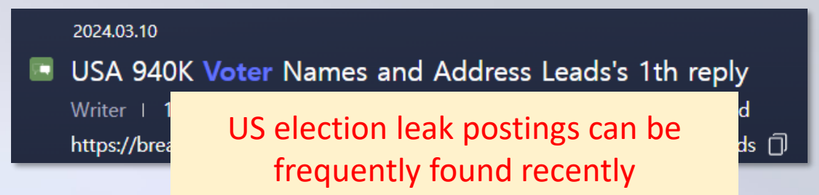
Dark web & Telegram
Weekly Highlights

May Week 2

California Voter Data Leaked and Publicly Released; Ongoing Election Data Breaches

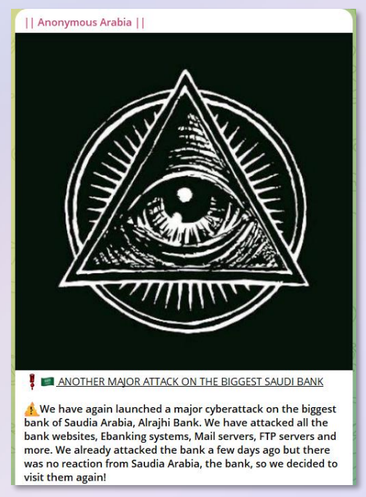
- On May 6th, a user named OriginalCrazyOldFart from the dark web hacking forum BreachForums leaked voter-related data from the San Jose area in California, making it publicly available for free.
- The leaked data, a file of approximately 200MB, includes voters' names, dates of birth, contact numbers, email addresses, and registration numbers. The data was leaked in 2018.
  - ✓ The user claims that due to the high cost of living in the area, which limits population movement, the data's reliability is high.
- With the U.S. presidential election approaching in November, voter information leaks and election-related posts have been frequently appearing on the dark web and Telegram.

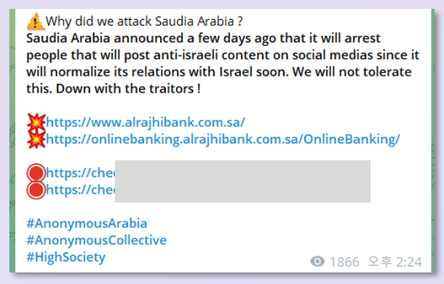




Major Islamic Bank Hit by Cyber Attack; Linked to Saudi's Israel Policy

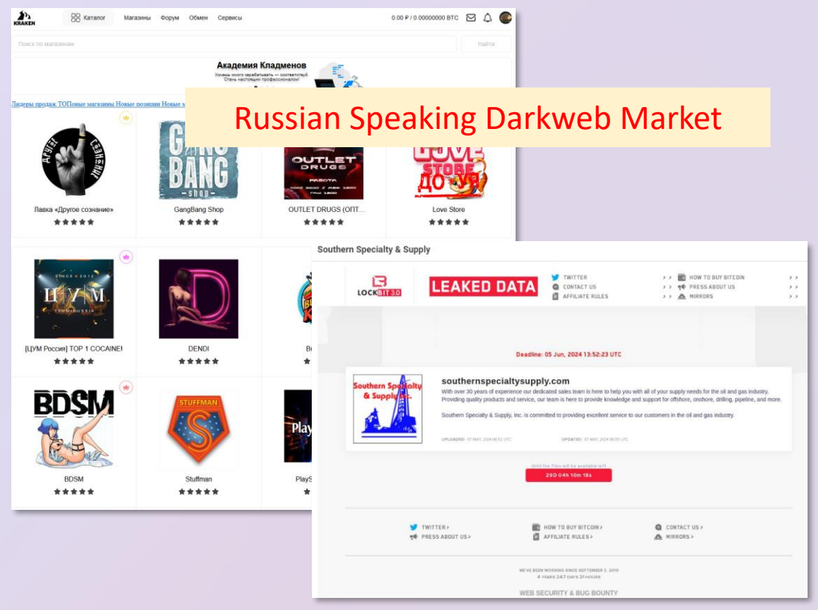
- Alrajhi Bank, a prominent bank in Saudi Arabia, was reportedly cyber-attacked due to international political motives, resulting in system damage.
- On May 6th, the hacking group Anonymous Arabia announced on their Telegram channel that they successfully attacked the bank, claiming to have damaged the institution's online banking, email, and FTP servers.
- The threat actor group cited the Saudi government's recent conciliatory policy towards Israel as the reason for the attack and hinted at potential future attacks on other institutions.





Dark Web Revives; Major Black Markets and Ransomware Groups Fuel 30% User Increase

- After a temporary decline following the rise of Telegram, the dark web ecosystem has shown signs of growth again this year.
- According to S2W data, the amount of collected dark web pages increased by about 50% from January to April compared to last year, and the daily average number of users on the dark web browser TOR also increased by approximately 30% globally.
- The recent increase in key dark web metrics is attributed to users who migrated to Telegram resuming dual activities on the dark web, the continued operations of ransomware gangs, and the emergence of major Russian black markets like Mega Market and Kraken Market.



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