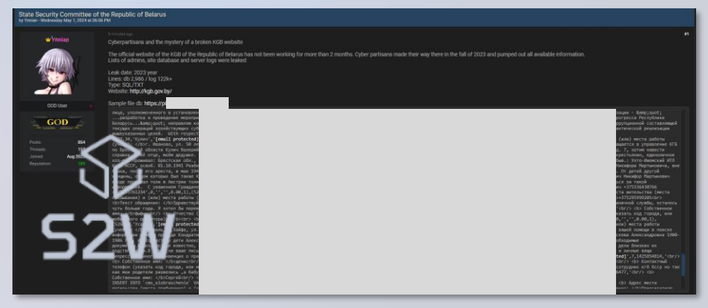
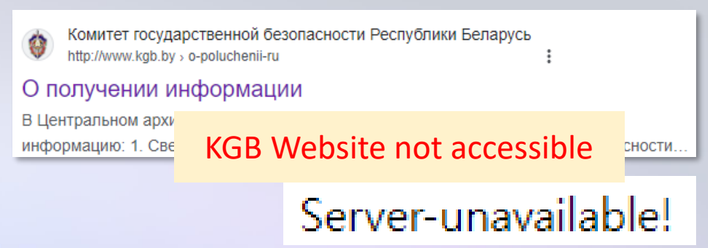
Dark web & Telegram
Weekly Highlights

May Week 1

Internal documents from the Belarus KGB website leaked

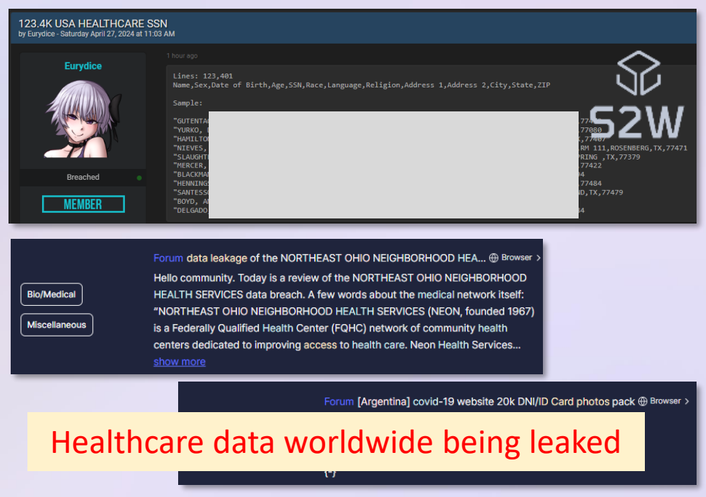
- Internal documents from Belarus's "KGB" security agency have leaked and are circulating on a dark web hacking forum.
- On May 1, a user named Ynnian on BreachForums posted details about the leak, including server logs and employee personal data.
- The incident was carried out by Cyber Partisans, a hacking group opposing Belarus's authoritarian regime, targeting government bodies.
- The post notes that the Belarus KGB website has been down for over two months, with the data breach occurring last fall.





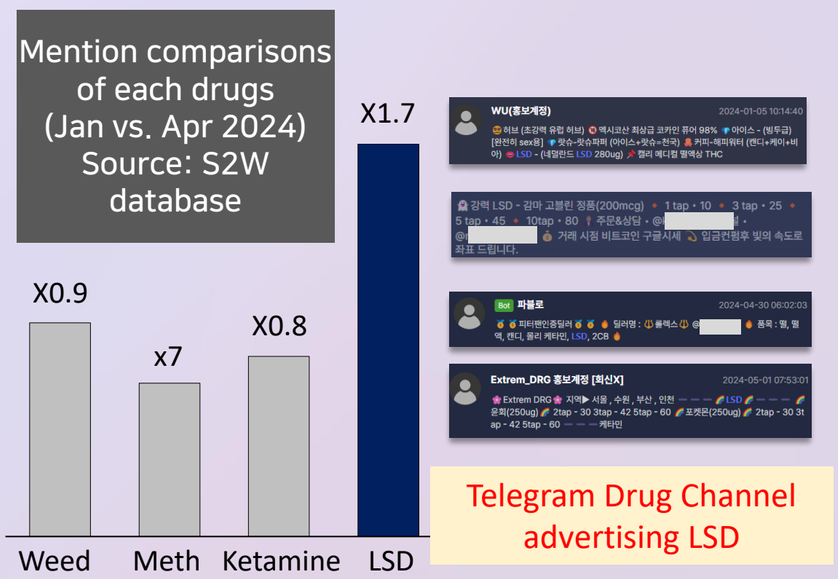
U.S. healthcare data breach detected on a prominent hacking forum

- Healthcare data containing U.S. consumers' Social Security numbers (SSN) has been leaked and shared on a dark web hacking forum.
- On April 27, a user named Eurydice on BreachForums leaked healthcare data of approximately 120,000 U.S. consumers, including names, genders, birthdates, SSNs, and addresses.
- Amid increasing cyber-attacks on the healthcare industry, the U.S. has been actively discussing enhanced cybersecurity measures for the sector, especially following a ransomware attack on UnitedHealth Group in February.



Mentions of LSD on Telegram drug channels have surged about 1.7 times in South Korea

- Since January, mentions of drugs on Telegram have slightly declined overall, but LSD, a major drug, has seen a significant rise.
- Data from S2W shows that while mentions of drugs like marijuana, methamphetamine, and ketamine increased last year and declined slightly starting January, LSD mentions have steadily risen, with a 1.7-fold increase by April.
- LSD, a potent hallucinogen, is distributed in paper form, making it hard to detect when mixed with mail or documents.



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