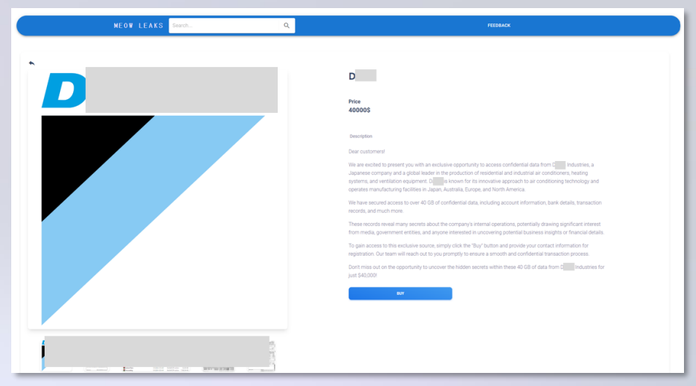
Dark web & Telegram
Weekly Highlights

July Week 4

Famous Japanese air conditioner maker D Company suffers internal data leak due to ransomware infection. Negotiations with the ransomware group likely failed.

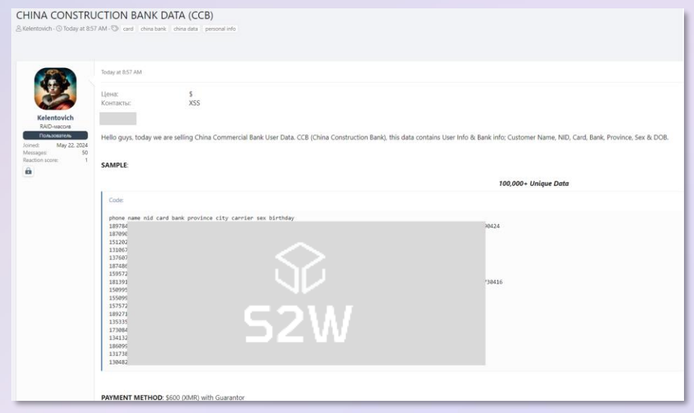
- D Company, famous for its air conditioners in Japan, has recently been infected with ransomware, leading to an internal data leak.
- On July 20, the dark web ransomware group MEOW LEAKS posted under D Company's name, claiming they had successfully extracted about 40GB of data from the affected company.
- They released some of the leaked data as samples, which included file lists, estimates, and documents that appeared to be contracts.



- The ransomware group is selling the company's internal data for approximately 50 million KRW, suggesting that negotiations with the affected company have failed.

China Construction Bank's internal data leaked. Detailed personal information of bank customers being sold.

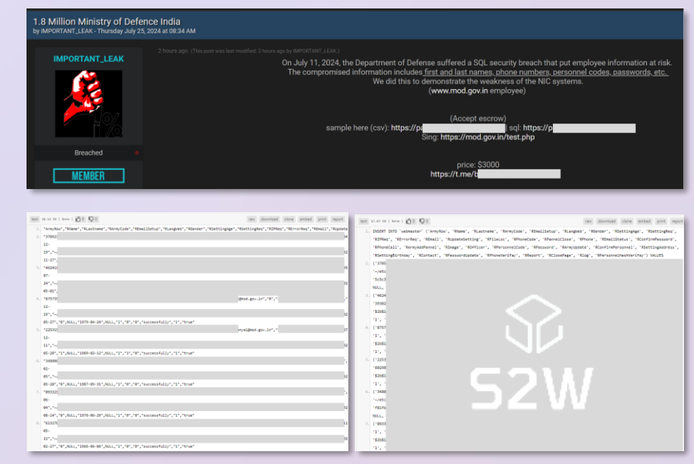
- Internal data from China Construction Bank (CCB) has been leaked and is being sold on the Russian hacking forum XSS.
- On July 22, an XSS threat actor named Kelentovich posted about selling CCB's internal data. According to the post, the leaked data includes detailed personal information of CCB customers, such as names, genders, birthdates, card information, and national identification numbers.



- As a sample of the leaked data, Kelentovich disclosed the personal information of about 20 Chinese individuals and set the selling price at approximately 800,000 KRW.

Indian Ministry of Defence employees' personal information, including IP addresses, leaked and up for sale.

- Internal data from the Indian Ministry of Defence has been leaked and is being sold on the dark web forum BreachForums.
- On July 25, a forum threat actor named IMPORTANT_LEAK posted about selling the personal information of 1.8 million Ministry of Defence employees. According to the post, the leaked data includes employees' names, contact details, identification codes, affiliations, and passwords.



- He also released a sample of the leaked data separately, which confirmed various personal information, identification codes, and passwords of individuals holding email accounts with the domain (mod.gov.in). Some of the data also included IP addresses.

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