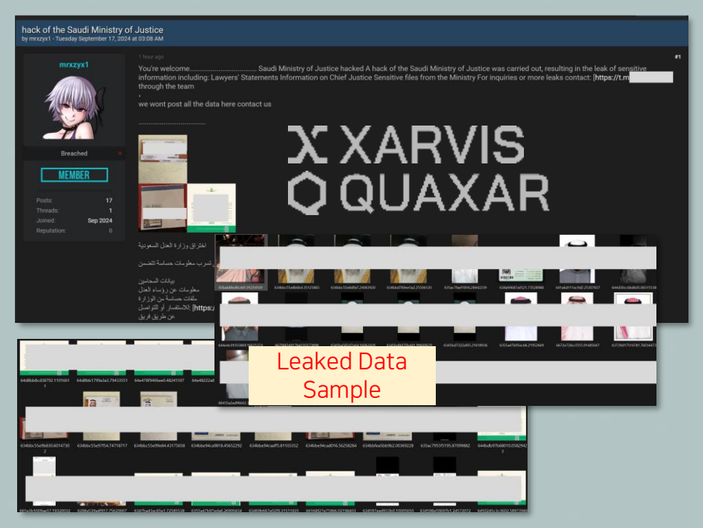
Dark web & Telegram Weekly Highlights

September Week 3

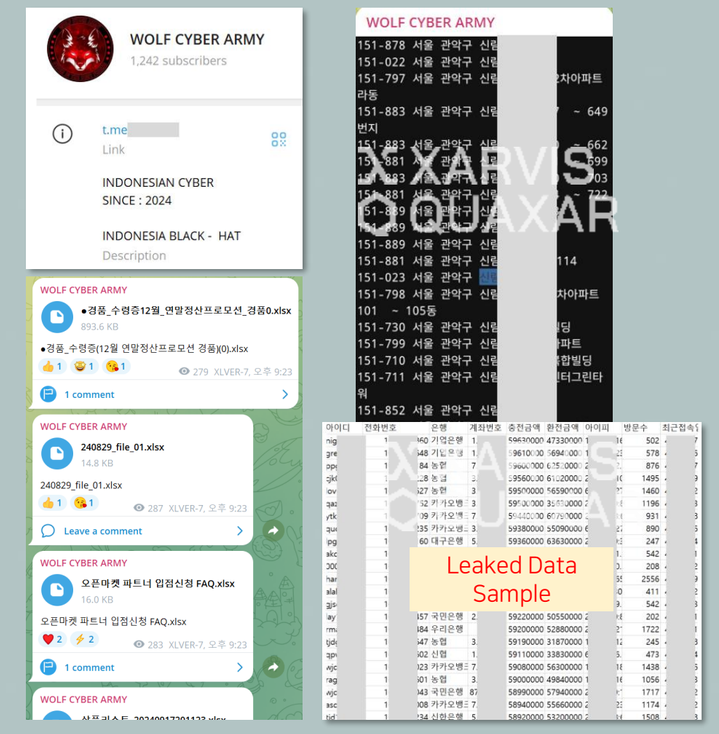
Saudi Justice Ministry Data Breach: Government IDs and Profiles Exposed

- A data breach from Saudi Arabia's Ministry of Justice has resulted in sensitive internal information being leaked and reportedly sold on the Darkweb forum, BreachForums.
- On September 17th, a threat actor using the alias "mrxzyx1" posted an offer to sell internal Saudi data, including samples of Saudi citizens' ID cards and official documents. A Telegram link was also provided.
- The Telegram link hosts additional sample files, including around 130 ID cards, government-issued documents, and profile pictures. The asking price for the data is set at $900.



Indonesian Hackers Target South Korean Websites, Data Leaked on Telegram

- Data from several South Korean websites has been leaked by Indonesian hackers and is being shared on Telegram.
- The hacking group "WOLF CYBER ARMY" shared around 10 Excel and text files via their Telegram channel on September 17th.
- Most data is from various sources and largely public or non-sensitive. However, some files contain sensitive information from illegal gambling sites, including contact details, bank accounts, transaction history, and IP addresses.
- The group, posing as Indonesian hackers, has been connected to recent South Korean data breaches, stressing the need for vigilance.



Bjorka Resumes Cyberattacks: Indonesian Tax Office Data Breach

- Bjorka, infamous for repeated cyberattacks on Indonesian government agencies, has re-emerged on BreachForums after an 8-month hiatus.
- After being inactive since January, Bjorka resumed activity on September 18th, leaking approximately 2GB of personal data belonging to Indonesian taxpayers for sale.
- The leaked data, about 2GB, includes names, identification numbers, contact details, and addresses, with the Indonesian President and his son reportedly among those affected.
- Bjorka's return has raised concerns about continued cyberattacks on Indonesian government institutions.

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