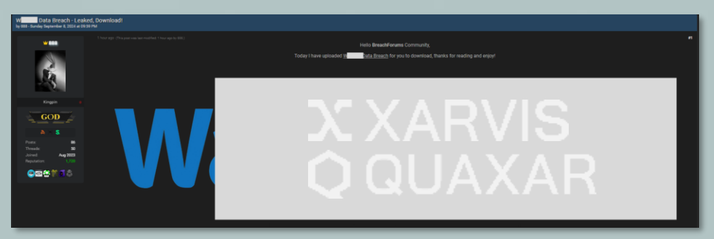
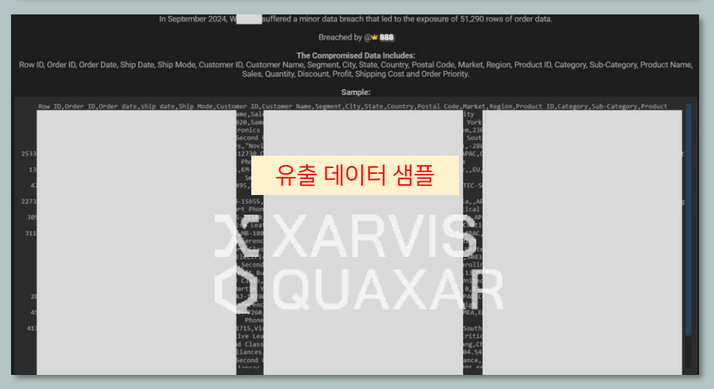
Dark web & Telegram Weekly Highlights

September Week 2

Data Leak Detected at Global Retail Giant W Company

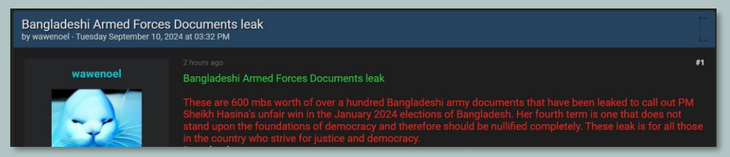
- Internal documents from the renowned U.S. retailer, Company W, were leaked and are currently being sold at a reduced price on the dark web forum BreachForums.
- On September 8, threat actor '888' announced the sale of data from W Company, taking personal responsibility for the breach. This recent attack compromised approximately 50,000 rows of data.
- The disclosed sample data includes comprehensive customer purchase details, such as names, addresses, items bought, product names, prices, and whether discounts were applied.

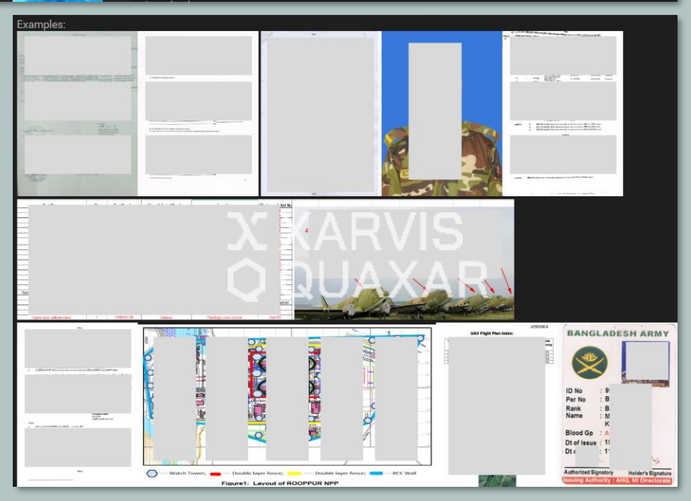




Bangladesh Military Information Compromised with Allegation of Election Fraud

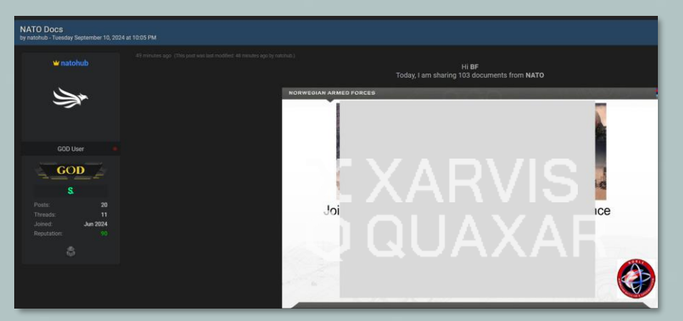
- On September 10, threat actor 'wawenoel' expressed their intention to sell internal documents from the Bangladesh military, amounting to about 600MB.
- The leaker references this year's January elections, accusing Prime Minister Sheikh Hasina of engaging in fraudulent activities to secure a fourth consecutive term.
- Exposed samples feature photos of military generals, IDs, military aircraft, areas presumed to be military zones, and various classified text documents.

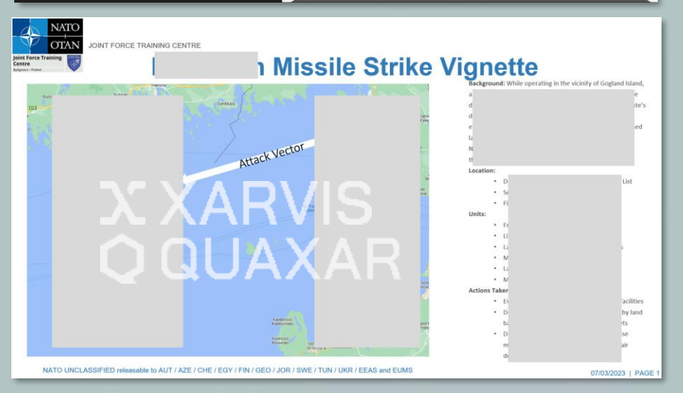




Sensitive NATO Documents Disclosed: Weapons and Operational Details Included

- Internal documents from NATO were leaked and are accessible on BreachForums.
- On September 10, threat actor 'natohub' uploaded "NATO docs," offering a free download link. The archive includes 103 files such as PowerPoint presentations, Excel spreadsheets, PDFs, and images.
- The documents unveiled provide specifics on weapons, systems, and numerous NATO military operations, some of which could create severe security risks if exposed. Natohub, active on the forum since 2022, has primarily shared leaks concerning military 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