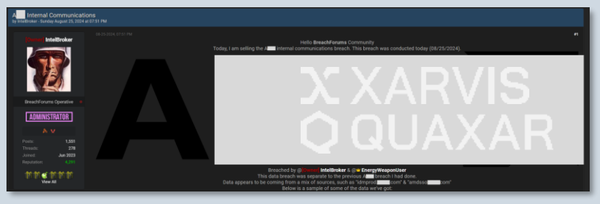
Dark web & Telegram
Weekly Highlights

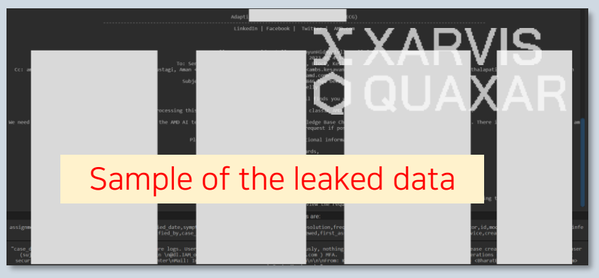
August Week 5

Data from American semiconductor company A was leaked again by the same hacker, including internal communications.

- Internal data from a well-known American semiconductor company, A, has been leaked and is being sold on the dark web hacking forum, BreachForums.



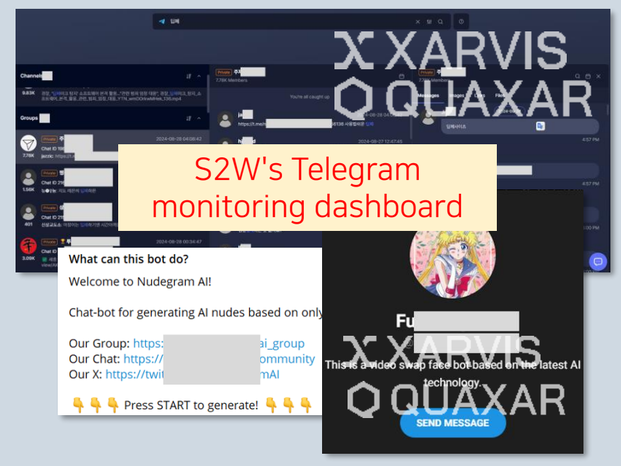
- According to the well-known forum hacker, IntelBroker, this leak involves new data that was leaked on August 25th and is different from the data leaked by the same hacker on June 17th. The leaked data reportedly includes a large number of internal communication messages from the company.



- A review of the sample released by the hacker shows numerous work-related messages exchanged between the company's internal employees, as well as what appears to be log records. This suggests that the leaked data may include dangerous information that could be exploited for a second attack.

Deepfake-related channels are actively being created on Telegram, with many detected through S2W's Telegram monitoring feature.

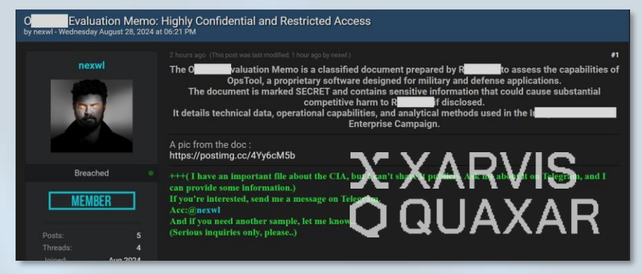
- As deepfake technology is increasingly being misused for sexual crimes targeting celebrities and ordinary people, there are ongoing signs of active creation of sexual crime channels on Telegram.
- S2W's Telegram monitoring has detected numerous posts sharing channels that either teach deepfake methods or offer services to create deepfake images or videos using provided photos. Many threat actorss in Korean channels are actively sharing these addresses.



- An analysis of the shared channel addresses shows that certain threat actors are repeatedly sharing multiple addresses. Given Telegram's ease of channel creation and movement, tracking these activities is expected to be challenging.

Information related to software developed by a major U.S. defense contractor has been leaked and detected for sale.

- A threat actor on the dark web hacking forum BreachForums claims to be selling leaked internal data related to military and defense software developed by the major U.S. defense contractor, company R.
- The forum threat actor 'nexwl' posted on August 28th, offering to sell data related to the performance evaluation of R's software, O*****. He claims that the leak could severely damage the company's competitiveness.



- The sample file he shared is an internal document from R, dated November of last year, marked as 'Confidential.' It also includes a warning that unauthorized disclosure outside the U.S. could result in legal consequences under international law. The hacker also claims to be selling CIA internal 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