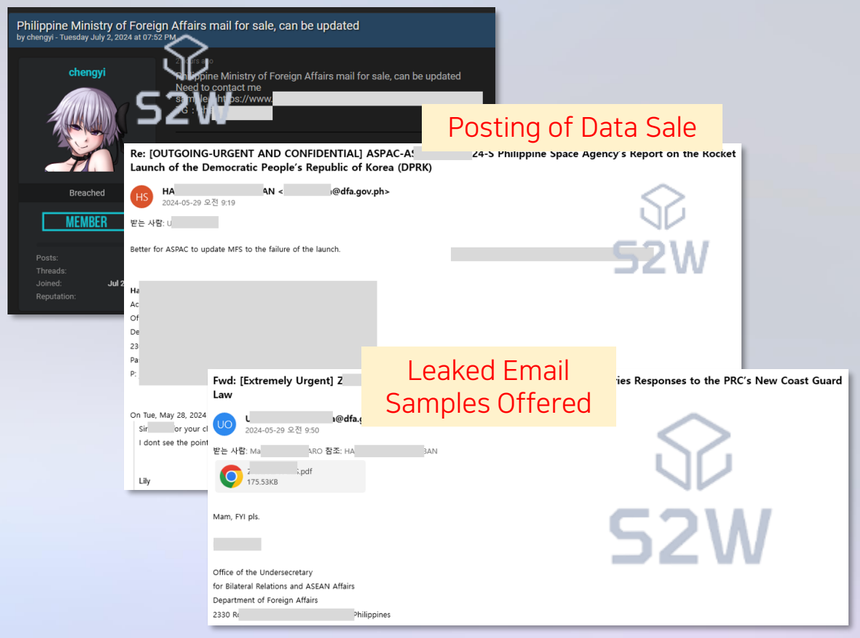
Dark web & Telegram
Weekly Highlights

July Week 1

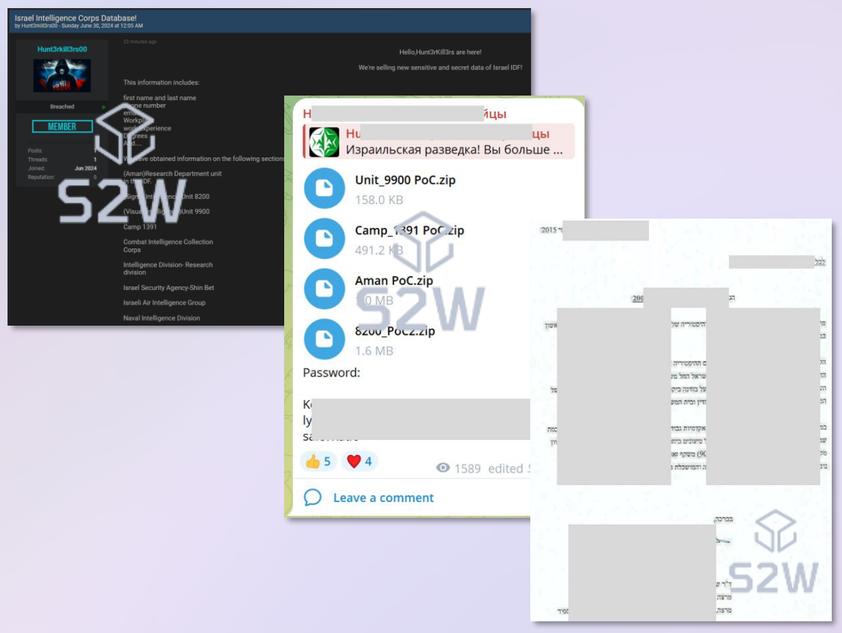
Confidential Philippine Foreign Ministry Emails Leaked, Highlighting North Korea-related Concerns

- Confidential materials from the Philippine Foreign Ministry have been compromised and are currently being sold on BreachForums.
- On July 2nd, a threat actor known as 'chengyi' listed email data from ministry staff for sale, providing 11 email chains as proof of the breach.
- An analysis of the samples reveals that communications from @dfa.gov.ph accounts discuss urgent and highly confidential issues related to North Korea, raising significant security concerns.



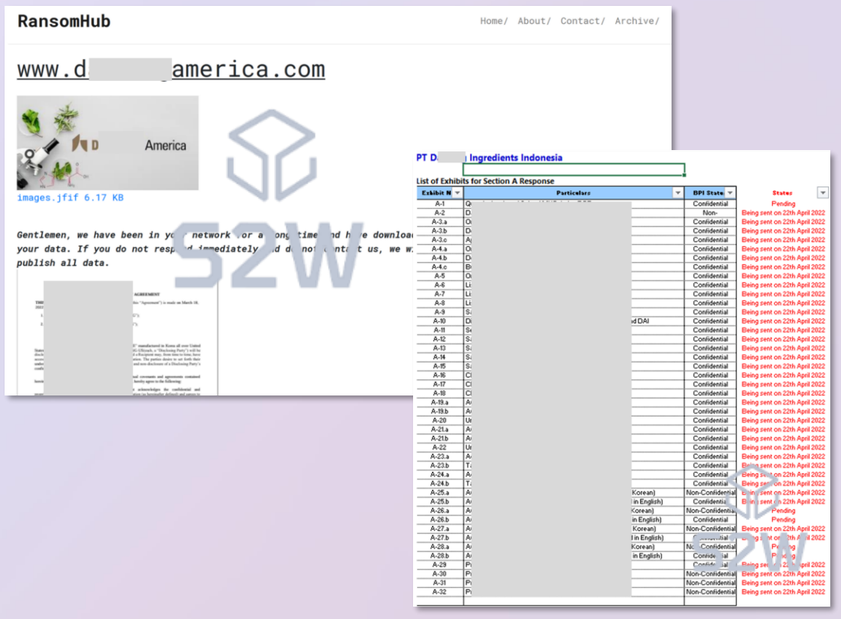
Israeli Intelligence Corps Document Leak Prompts Security Alarms

- On June 30th, internal documents from the Israeli Intelligence Corps were posted for sale on BreachForums.
- The threat actor, Hunt3rkill3rs00, claimed to have leaked data including personal details of defense personnel and classified documents.
- Samples reviewed on a Telegram channel managed by the threat actor show numerous documents in Hebrew, marked as internal or confidential, underscoring the breach's severity.



Ransomware Attack Compromises Sensitive Data at U.S. Branch of Korean Food Company

- Recent evidence indicates that the U.S Branch of a notable Korean food company has suffered a ransomware-induced data breach.
- On July 3rd, the darkweb ransomware group Ransomhub published samples of the stolen data on their leak site, explicitly naming the affected the Korean Company, D******.
- The compromised entity, identified as D's U.S. branch, had materials leaked including invoices, contracts, and document lists, all explicitly marked as 'confidential'.



S2W

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