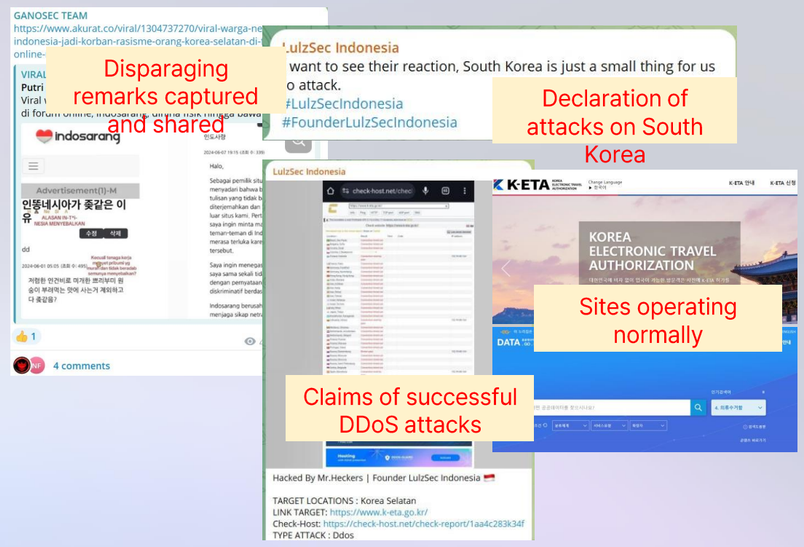
Dark web & Telegram
Weekly Highlights

June Week 2

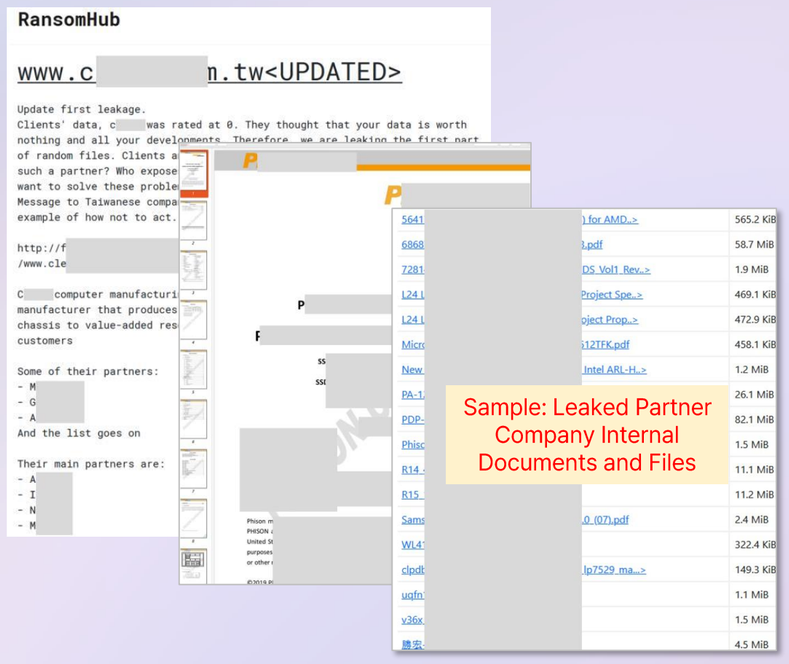
South Korean Government Sites Face Indonesian DDoS Attacks but Maintain Normal Operations

- On June 11, the Indonesian hacking group GANOSEC TEAM reported via their Telegram channel that a Korean community in Indonesia had made disparaging remarks about Indonesia.
- This message spread among Indonesian hackers, prompting the hacktivist group named Lulzsec Indonesia to declare their intention to carry out a cyber attack against South Korea.
- Lulzsec Indonesia claimed to have successfully executed DDoS attacks on South Korean government entities and the involved Korean Community. However, subsequent checks confirmed that these websites were operating normally.



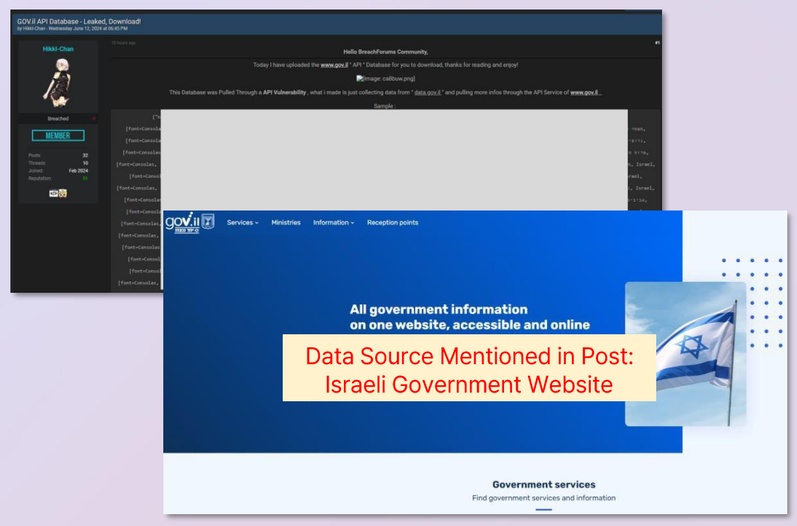
Ransomware Strikes Taiwanese Computer Manufacturer, Uses Partner Data for Extortion Attempts

- Taiwanese computer manufacturer, Company named C, confirmed a ransomware infection resulting in data leakage (initial posting on May 29, data leak posting on June 13).
- On June 13, the ransomware group RansomHub published some of Company C's data to pressure them. The group used leaked partner data for extortion, which the victim company refused to pay.
- Analysis of the disclosed data revealed filenames that includes US and Taiwanese semiconductor companies, as well as Korean Companies.



Israeli Government Agency Data Leaked Due to API Vulnerability

- On June 12, a breach was reported on BreachForums that disclosed internal data from an Israeli government agency.
- A threat actor, known as Hikkl-Chan, exploited a vulnerability in the API of a website managing Israeli public data, resulting in the leakage of various data sets, including those published.
- The exposed samples include names, contact details, birthdates, identity numbers, and addresses of presumed Israeli citizens, documented in both English and Hebrew. The breach impacted approximately 270,000 entries.



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