Dark web & Telegram Weekly Highlights

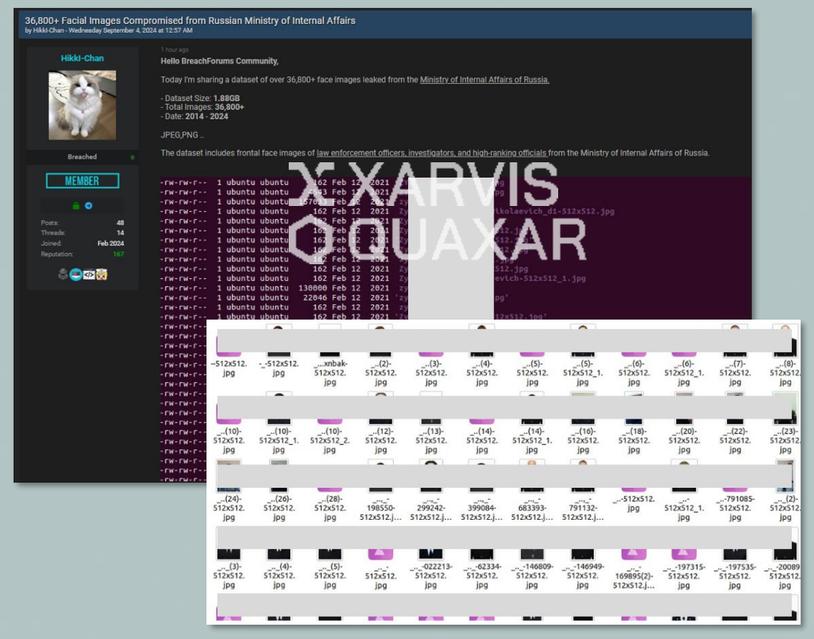
September Week 1

Renowned Electronics Manufacturer Hit by Ransomware, Suffers Data Breach

- Company S, headquartered in Japan and transitioning from camcorders and batteries to AV devices, has reported significant data leakage due to a ransomware attack.
- On September 2, RansomHub claimed to have leaked approximately 500GB of data from the company's Taiwan branch.
- Released samples include product blueprints, factory layouts, and testing reports, suggesting the potential compromise of recent documents.

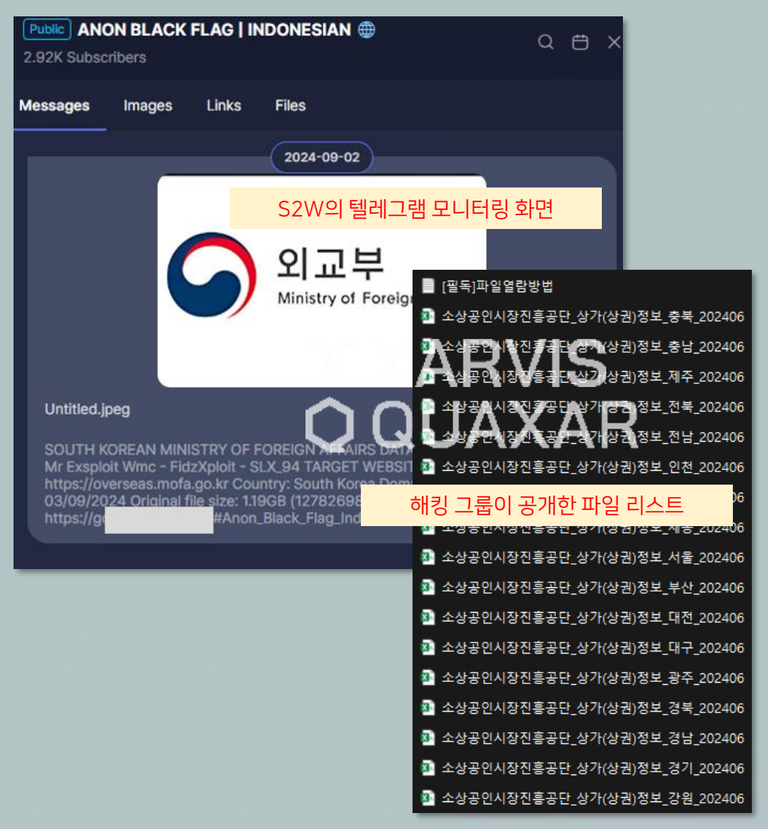
Personal Data of 37,000 Russian Ministry Employees Exposed Online

- Personal and ID photos of employees from the Russian Ministry of Internal Affairs are being disseminated on the BreachForums.
- On September 4, threat actor Hikkl-Chan posted approximately 37,000 images totaling 2GB, with data ranging from 2014 to the present.
- Analysis of the sample data confirms it includes image files named after employees and bust shot ID photos of those presumed to be Ministry staff.



Indonesian Hackers Claim to Breach South Korean Foreign Affairs Ministry

- An Indonesian hacking group active on Telegram claims to have successfully breached and leaked data from South Korea's Ministry of Foreign Affairs.
- The group, ANON BLACK FLAG Indonesia, reported on September 2 that it had obtained about 1.2GB of data, providing samples for verification.
- The leaked samples contain market data from 17 regions in Korea, managed by the Korea SMEs and Startups Agency, including shop names, industries, and locations.
- This group has intensified attacks on Korean entities following derogatory remarks about Indonesians noted in a Korean online community in June.



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