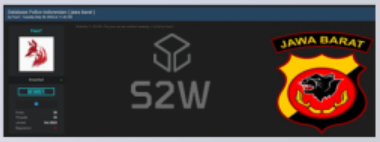
Dark web & Telegram
Weekly Highlights

March Week 5

Significant Data Leak Involving Indonesian Police Officers Raises Security Concerns

- On May 28th, a threat actor identified as Foxs7 on the dark web forum BreachForums advertised a data set involving West Java, Indonesia police officers.
- The data set includes personal details of about 26,000 officers, such as names, contact info, ranks, and affiliations, with a sample for 70 officers provided.
- Offered at approximately 700,000 KRW ($500), the potential exploitation of this data poses significant risks such as privacy intrusions, impersonation of officers, and targeted assaults against law enforcement personnel.



1.5TB Data Breach at U.S. Medical Company, Server Access Still Unsecured

- On May 29th, a threat actor known as Ddarknotevil on the Russian dark web forum XSS disclosed the sale of data from a healthcare provider that operates more than 50 facilities in the U.S.healthcare provider operating over 50 facilities.
- The seller disclosed that the substantial data breach involved 1.5TB, comprising patients' personal and medical records, sourced from the company's FTP server.
- Additionally, the seller mentioned that the data continues to be updated daily by the healthcare provider, suggesting that the hacking group retains ongoing access to the server, unbeknownst to the company.

Malaysian government agency's data sale caught amid rising hacking trend targeting Malaysia

- On March 7th, BreachForums showcased a sale of ilmia.gov.my's databases and access rights by haxormy1337.
- The data sample, priced at $170, included detailed user info.
- With recent breaches involving Malaysian agencies and corporations, national proactive steps are essential.

S2W