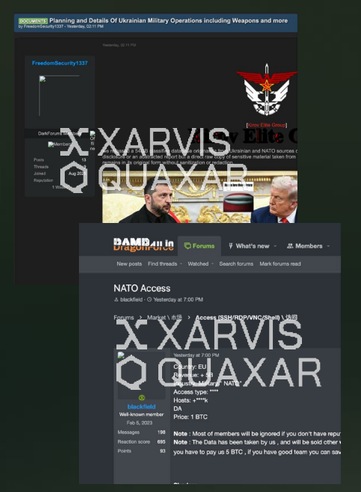
Weekly Darkweb

AI-Based Big Data Analysis

August Week 4

NATO Faces Continued Cyberattacks, Suspected Data Leaks on Hacking Forum

- [8/21] A post sharing classified documents related to Ukraine and NATO from the past eight years was detected on the dark web hacking forum “DarkForums.”



➢ The user claimed the data consisted of original copies stolen from secure servers and internal repositories, including sensitive information such as Ukraine’s defense and operational plans and NATO’s cooperation structure. The 53GB file was shared through a dark web link, now inactive.

- [8/27] A post offering NATO system access credentials and associated data was detected on the dark web hacking forum “RAMP.”

➢ According to the seller, the exfiltrated data contains information on an organization tied to Israel’s weapons supply chain and holds strategic value for Iran. System access credentials were priced at 1 BTC; the full package, including data, at 5 BTC. The seller emphasized that their past military and government access sales were known for durability.

Japanese Resident Data From ‘e-Stat’ Reportedly Leaked on Dark Web

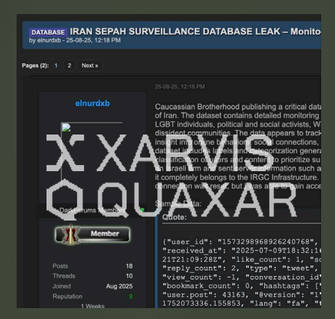
- On August 28, a user known as ‘DigitalGhostt’ was found selling personal data of Japanese residents, allegedly leaked from the government statistics portal ‘e-Stat,’ on “DarkForums” and a Telegram channel.

- The user claimed the data contains sensitive information on 78 million Japanese, including phone numbers, email addresses, names, and home addresses, and posted sample records as proof.

- S2W’s profiling tool shows the user began selling leaked data in late June through Telegram-based hacking communities and DarkForums, and has been actively operating Telegram channels ‘RU Ghost_Market RU’ and ‘RU DigitalGhost RU’ since August 2.

Iranian IRGC Surveillance Data Allegedly Found on Hacking Forum

- On August 25, a post was identified on “DarkForums” claiming that surveillance program data operated by Iran’s Islamic Revolutionary Guard Corps (IRGC) had been leaked.



  - ✓ In July, the Telegram channel ‘Caucasian Brotherhood’ distributed a classified dataset called ‘FSBTool,’ which was found to contain user IDs, names, phone numbers, and email addresses.

- User ‘elnurdxb’ allegedly identified the ‘FSBTool’ as part of IRGC infrastructure after personally confirming server details with an Israeli company. The data was found to include X (formerly Twitter) activity and personal details of targeted groups such as political activists, Azerbaijani nationals, and opposition communities, with labels marking surveillance priority levels.

- The user published a 6.5MB file with sample data that included activity on X and assigned labels related to certain individuals.