GlobalResearch
Center for Research on Globalization

US Officials Allege Israel Behind Cyberattack on Iranian Gas Stations

By Israel Hayom
Global Research, December 02, 2021
Israel Hayom 28 November 2021

Region: Middle East & North Africa
Theme: Intelligence

***

Iranian officials with knowledge of the investigation, meanwhile, tell the NY Times that the hackers also seized control of the ministry's fuel storage tanks and may have gained access to data on international oil sales, a state secret that could expose how Iran evades international sanctions.

Israel was behind a cyberattack on Iran's nationwide fuel distribution system in late October that paralyzed the Islamic republic's 4,300 gas stations, two US defense officials speaking on condition of anonymity told the *New York Times* over the weekend.

The attack came on the heels of previous cyberattacks in recent months, which shut down vital services and infrastructure in Iran – from disruptions to traffic lights and train services to water and electric supplies.

No one assumed responsibility for disabling the gas stations or for the previous attacks in Iran. In Tehran, too, officials were careful not to point a finger at the "usual suspects," although Iranian **President Ebrahim Raisi** said that a country with cyber-capabilities wanted to "make people angry by creating disorder and disruption." The foreign and Israeli press had already attributed the cyberattacks to Israel, saying their objective was to apply pressure on the Iranian regime and stall its nuclear progress.

In response to the alleged Israeli attack, the Iran-affiliated hacker group "BlackShadow" hacked the servers of Israeli internet company Cyberserve. The hackers shuttered the company's servers and threatened to leak data pertaining to hundreds of thousands of users.

Cyberserve is a web hosting company that provides servers and data storage for companies such as *Kan* public broadcaster, the Israel Lottery, Birthright, the Dan and Kavim public transportation companies, the Children's Museum in Holon, LGBTQ dating app "Atraf," tour booking company Pegasus, the Israeli Children's Museum, and dozens of other sites.

Israel also accused Iran of carrying out a cyberattack in early April on a minor water facility that sought to poison the water supply delivered to hundreds of thousands of homes in the greater Tel Aviv area.

Meanwhile, to get pumps back online, the *NY Times* reported, Iran's Oil Ministry had to send technicians to every gas station in the country. Once the pumps were reset, most stations could still sell only unsubsidized fuel, which is twice the price of subsidized fuel.

It took nearly two weeks to restore the subsidy network, which allots each vehicle 60 liters (about 16 gallons) a month at half price.

The alleged Israeli hack, however, may have been more serious than an inconvenience to motorists, the *NY Times* report speculated.

A senior manager in the Oil Ministry and an oil dealer with knowledge of the investigation, who spoke to the *NYT* on the condition of anonymity "to avoid repercussions" said that officials were alarmed that the hackers had also seized control of the ministry's fuel storage tanks and may have gained access to data on international oil sales – a state secret that could expose how Iran evades international sanctions.

According to the *NYT*, because the oil ministry's computer servers contain such sensitive data, the system operates unconnected to the internet, leading to suspicions among Iranian officials that Israel may have had inside help.

Three senior Israeli officials, who asked not to be identified in order to discuss secret cyber issues, told the *NY Times* that Black Shadow was either part of the Iranian government or freelance hackers working for the government.

*

Note to readers: Please click the share buttons above or below. Follow us on Instagram, @crg_globalresearch. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.
