

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](#)

All Global Research articles can be read in 51 languages by activating the “Translate Website” drop down menu on the top banner of our home page (Desktop version).

To receive Global Research’s Daily Newsletter (selected articles), [click here](#).

Visit and follow us on Instagram at [@crg_globalresearch](#).

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.

The original source of this article is [Israel Hayom](#)

Copyright © [Israel Hayom](#), [Israel Hayom](#), 2021

[Comment on Global Research Articles on our Facebook page](#)

[Become a Member of Global Research](#)

Articles by: [Israel Hayom](#)

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca