Iran oil sector hit by 'cyber attack'

April 23 2012, by Mohammad Davari

A voracious virus attack has hit computers running key parts of Iran's oil sector, forcing authorities to unplug its main oil export terminal from the Internet and to set up a cyber crisis team, according to reports.

A voracious virus attack has hit computers running key parts of Iran's oil sector, forcing authorities to unplug its main oil export terminal from the Internet and to set up a cyber crisis team, according to reports on Monday.

The Mehr news agency reported that Iran's principal oil terminal on Kharg island in the Gulf has been disconnected from the Internet since Sunday along with facilities in other parts of the country.

The Kharg terminal handles 90 percent of Iran's oil exports, according to the National Iranian Oil Terminals Company.

Mehr said the Internet disconnection "has not caused any problem" in oil production and exports.

Mehr did not give a source for the report, and no official Iranian media confirmed the information.

The websites of the Iranian oil ministry (www.mop.ir) and the National Iranian Oil Company (www.nioc.ir) were off-line for hours after they and other affiliated official sites were brought down by the malware, Mehr and other news agencies including Fars and ISNA said.

By late Monday, the ministry website was back up, though the NIOC site remained down.

Oil ministry spokesman Alireza Nikzad told the ministry's news website SHANA that, contrary to initial reports in Iran, the virus had succeeded in wiping data off official servers.

"To say that no data was harmed is not right. Only data related to some of the users have been compromised," he said.

Iran's oil ministry has set up a "cyber crisis committee" to confront the "cyber attack," Mehr said, quoting a civil defence official at the ministry.

Iran's reaction to the virus attack was a test of procedures put in place after the country suffered a massive cyber assault in 2010 by a worm called Stuxnet that reportedly dealt a big blow to the country's nuclear programme.

Stuxnet, Western media and experts said, homed in precisely on computers running uranium enrichment centrifuges at Iran's nuclear facility in Natanz, destroying thousands of them and setting the atomic

programme back months.

Tehran has disputed the extent of the damage caused, and has in any case, according to the International Atomic Energy Agency, since recovered and redoubled its uranium enrichment acitivities.

The highly sophisticated code in Stuxnet, and an apparent "expiry" procedure meant to render it harmless after a period of time, suggested to Western anti-virus experts that it could only have been created by a government.

Suspicion has focused on the United States, with or without help from Israel.

Washington and Tel Aviv are the loudest critics of Iran's nuclear programme, which they see as masking a bid to develop the capability to make atomic weapons.

Iran, which denies its nuclear programme is anything but peaceful, has come under intense Western pressure in recent months in the form of economic sanctions aimed at curbing its all-important oil exports.

The Islamic republic is OPEC's second-biggest exporter, after Saudi Arabia, and relies on crude sales for 80 percent of its foreign currency and for more than half of its government finances.

The issues of Tehran's nuclear activities and Western sanctions are being raised in talks between Iran and world powers that were revived in Istanbul this month and are due to continue in Baghdad on May 23.

https://phys.org/news/2012-04-iran-oil-sector-cyber.html