Saudi Aramco says most damage from computer attack fixed

Daniel Fineren and Amena Bakr, Reuters

(Reuters) - Saudi Aramco, the world's biggest oil producer, has resumed operating its main internal computer networks after a virus infected about 30,000 of its workstations in mid-August, the company said on Sunday.

Immediately after the August 15 cyber attack, the company announced it had cut off its electronic systems off from the outside world to prevent further attacks.

On Sunday, Saudi Aramco said the workstations had now been cleansed of the virus and restored to service. Oil exploration and production were not affected because they operate on isolated systems, it said.

"We would like to emphasize and assure our stakeholders, customers and partners that our core businesses of oil and gas exploration, production and distribution from the wellhead to the distribution network were unaffected and are functioning as reliably as ever," CEO Khalid al-Falih said in a statement.

However, one of Saudi Aramco's websites which was taken offline after the attack -- www.aramco.com -- remained down on Sunday. Emails sent by Reuters to people within the company continued to bounce back.

The company said the virus "originated from external sources," and that an investigation into the causes of the incident and those responsible were continuing. It did not elaborate.

Information technology experts have warned that cyber attacks on countries' energy infrastructure, whether conducted by hostile governments, militant groups or private "hacktivists" to make political points, could disrupt energy supplies.

Iran [1], the target of international economic sanctions on focused on its oil industry over its disputed nuclear program, has been hit by several cyber attacks in the last few years.

In April, a virus targeted the Iranian oil ministry and national oil company networks, forcing Iran to disconnect the control systems of oil facilities including Kharg Island, which handles most of the country's crude exports.

Iran has attributed some of the attacks to the United States, Israel and Britain.

Current and former U.S. officials told Reuters this year that the United States built the complex Stuxnet computer worm to try to prevent Tehran from completing suspected nuclear weapons work.

POSTING

An English-language posting on an online bulletin board on August 15, signed by a group called the "Cutting Sword of Justice," claimed the group had launched the attack to destroy 30,000 computers at Saudi Aramco.

It said the company was the main source of income for the Saudi government, which it blamed for "crimes and atrocities" in several countries, including Syria [2] and Bahrain. Saudi Arabia sent troops into Bahrain last year to back the Gulf state's Sunni Muslim rulers against Shi'ite-led protesters. Riyadh is also supporting Sunni rebels against the Syrian regime of President Bashar al-Assad.

Before this month's attack, the Cutting Sword of Justice was not widely known, and information security experts contacted by Reuters had no information on the group.

Rob Rachwald, director of security for U.S.-based data security firm Imperva, said in a blog posting last week that if the Saudi Aramco attack was carried out by hacktivists, it could be a milestone in computer hacking.

"A group of hobbyists and hacktivists with several very strong-minded developers and hackers achieved results similar to what we have allegedly seen governments accomplish," Rachwald wrote.

Symantec, one of the world's largest internet security companies, said on the day after the Saudi Aramco attack that it had discovered a new virus that was targeting at least one organization in the global energy sector, although it did not name that organization.

"It is a destructive malware that corrupts files on a compromised computer and overwrites the MBR (Master Boot Record) in an effort to render a computer unusable," Symantec said in a blog posting about the virus, which it called W32.Disttrack. "Threats with such destructive payloads are unusual and are not typical of targeted attacks."

Saudi Aramco's Al-Falih said in his statement on Sunday: "Saudi Aramco is not the only company that became a target for such attempts, and this was not the first nor will it be the last illegal attempt to intrude into our systems, and we will ensure that we will further reinforce our systems with all available means to protect against a recurrence of this type of cyber attack."

(Additional reporting by Reem Shamseddine and Angus McDowall, editing by Andrew Torchia and Anna Willard; desking by Gary Crosse)

Links:
[1] http://www.reuters.com/places/iran
[2] http://www.reuters.com/places/syria