Saudi Arabia warns destructive computer virus has returned (Update)

24 January 2017, by Jon Gambrell

Saudi Arabia is warning that a computer virus that destroyed systems of its state-run oil company in 2012 has returned to the kingdom, with at least one major petrochemical company apparently affected by its spread.

Suspicion for the initial dispersal of the Shamoon virus in 2012 fell on Iran as it came after the Stuxnet cyberattack targeting Tehran's contested nuclear enrichment program.

It wasn't immediately clear who could be responsible for the new infection, though the relations between regional rivals remain tense.

A report Monday by Saudi state-run television included comments suggesting that 15 government agencies and private institutions had been hit by the Shamoon virus, including the Saudi Labor Ministry. The ministry said it was working with the Interior Ministry to contain the virus.

Sadara, a joint venture between the Saudi Arabian Oil Co. and Michigan-based Dow Chemical Co., shut down its computer network Monday over a disruption.

Company spokesman Sami Amin said its network remained down Tuesday, though it hadn't affected operations at the facility. He declined to comment further.

Sadara is based in Jubail Industrial City, which sits about 100 kilometers (60 miles) northwest of the eastern Saudi city of Dammam in the heartland of the kingdom's oil industry. The $20 billion facility, inaugurated by Saudi King Salman in late November, includes 26 manufacturing units that will produce more than 3 million metric tons of plastics and chemical products.

Another state-run TV report on Tuesday said the Saudi Technical and Vocational Training Corp. was affected, though a spokesman denied the virus did any damage to its network.

Symantec Corp., a California-based security firm, warned in late November that Shamoon had been spotted again in Saudi Arabia. Computers affected had their hard drives erased and displayed a photograph of the body of 3-year-old Syrian boy Aylan Kurdi, who drowned fleeing his country's civil war, Symantec said.

"Why Shamoon has suddenly returned again after four years is unknown," Symantec said . "However, with its highly destructive payload, it is clear that the attackers want their targets to sit up and take notice."

The November attacks apparently involved previously stolen passwords. Symantec on Monday said the outbreak might be linked to a group it called Greenbug, which previously attacked targets in Bahrain, Iran, Iraq, Kuwait, Qatar, Saudi Arabia and Turkey with emails carrying malicious attachments.

Shamoon, named for a folder in its code, first emerged in Saudi Arabia in 2012. In that attack, which hit Saudi Aramco and Qatari natural gas producer RasGas, the virus deleted hard drives and then displayed a picture of a burning American flag on computer screens. The attack forced Saudi Aramco to shut down its network and destroyed over 30,000 computers.

"All told, the Shamoon virus was probably the most destructive attack that the private sector has seen to date," then-U.S. Defense Secretary Leon Panetta said at the time.

Shortly before Panetta's speech, a former U.S. official told The Associated Press that American officials firmly believed Iranian hackers likely backed by Tehran were responsible for the attack.

Iran denied being responsible for the 2012

Shamoon outbreak. Tehran had no immediate comment on the new outbreak.

The first emergence of Shamoon came as Iran faced international sanctions over its contested nuclear program and after it saw thousands of centrifuges destroyed by the Stuxnet virus, widely believed to be an American and Israeli creation.

Last year, a series of fires at Iranian petrochemical plants and facilities have raised suspicions about hacking potentially playing a role.

Hostilities persist between Shiite power Iran and Sunni-ruled Saudi Arabia.

The countries support opposite sides in the wars gripping Syria and Yemen, while the kingdom has backed Bahrain's Sunni rulers amid a crackdown on dissent on the Shiite-majority island.

Saudi Arabia severed diplomatic relations with Iran last year after protesters there—angry about its execution of a Shiite cleric—stormed two Saudi diplomatic posts.

APA citation: Saudi Arabia warns destructive computer virus has returned (Update) (2017, January 24) retrieved 6 March 2021 from https://phys.org/news/2017-01-saudi-arabia-destructive-virus.html