Virus origin in Gulf computer attacks in question

September 4 2012, by Adam Schreck

In this Tuesday, Dec. 4, 2007 file photo, Employees of the Saudi Aramco oil company prepare for the first day of the Arab Oil and Gas exhibition in Dubai, United Arab Emirates. Computer security technicians are still trying to unravel how destructive viruses crippled two major Arab energy companies in recent weeks, but early indications suggest the infections were the result of a highly targeted and possibly coordinated sabotage attack. While pinpointing culprits in the shadowy world of cyber crime is tricky, some experts believe Iran itself the victim of computer attacks may have played a role. Others aren't so sure. (AP Photo/Kamran Jebreili, File)

(AP)—Security technicians are beginning to suspect that highly targeted virus attacks were behind the recent crippling of computer systems at two major Gulf energy companies, even as questions swirl about the source of the strikes.

The computer disruptions at state oil giant Saudi Aramco and Qatari natural gas producer RasGas do not appear to have affected oil and gas production. Yet they highlight another risk to the security of energy supplies in the Persian Gulf region.

Neither company has said how much data may have been lost, but the scope of the attacks appears extensive. Aramco blocked all its electronic systems from outside access for several days to deal with the problem, which it says affected about 30,000 workstations last month. RasGas technicians were still working to fix that company's systems more than a week after being hit.

Although pinpointing culprits in the shadowy world of Internet crime is tricky, some experts believe that Iran—itself the victim of multiple computer attacks—may have played a role. Others aren't so sure, saying there isn't enough evidence. That may be partly by design, as the virus thought to be involved in at least one of the attacks covers its tracks by erasing data on computer hard drives.

The attacks may not be over. Security and data storage company Symantec said this week that it is investigating reports of additional infections involving the virus at the center of what security experts refer to as the Shamoon attacks. It's widely believed to be responsible for the Aramco disruption, and several security experts suspect it in the Qatar attack.

The virus can spread through networked computers and ultimately wipes out files by overwriting them—sometimes leaving behind an image of a burning American flag.

Aviv Raff, the chief technology officer of Israeli computer security firm Seculert, said other companies outside the energy industry have also been affected, though confidentiality agreements prevent him from

providing details.

Saudi Aramco revealed that its network was infected on Aug. 15 when it announced it was disconnecting all its computer systems from outside access.

Two previously unknown groups immediately claimed responsibility for the Aramco attack in statements posted to a website often used by computer hackers. One of the groups, the Cutting Sword of Justice, said it was avenging what it called Saudi support for "crimes and atrocities" in Syria, Bahrain and other Arab countries.

Aramco said late last month that it had managed to restore all network services after cleaning computers affected by what it called "a malicious virus that originated from external sources." Key oil exploration and production operations had been unaffected because they use isolated computer networks, it said.

Unlike viruses that aim to hit as many targets as possible, this one appears designed to cripple computers on specific networks identified by the culprits, said Bulent Teksoz, chief security strategist for emerging markets at Symantec. He declined to name the affected organizations.

Some researchers, such as Raff, suspect the memory-wiping mechanism was simply a way to remove evidence of earlier incursions, during which hackers might have stolen information or rerouted network traffic.

Last week, Qatar's RasGas disclosed an Aug. 27 attack by an unknown virus on its office computer systems. Technicians were still working to get the system running again. RasGas, a partnership between state-run Qatar Petroleum and U.S. oil giant Exxon Mobil Corp., said gas production has not been affected.

Exxon Mobil spokeswoman Adrienne Fleming declined to comment on the virus or whether the oil company itself had been hit, citing a company practice of not discussing security issues.

Even less is known about the RasGas infection. Like Aramco, the company has not publicly identified the virus responsible. But several security experts suspect the attacks are related, given the timing and the apparent similarity of the infections.

"My guess would be that it was another Shamoon attack," said Jeffrey Carr, the head of Taia Global, a computer security firm in McLean, Virginia.

Carr believes hackers working on behalf of the Iranian government were behind both attacks. He notes similarities between Shamoon and a virus that previously struck Iran, suggesting that Iran-linked hackers may have created Shamoon by adapting computer code from the earlier virus.

A number of Iranian groups have the skills to carry out an attack of this scope and may be using false claims of responsibility to obscure Tehran's involvement, he said.

Iranian officials have not commented publicly on the latest viruses to hit the region. But Iran appears to be building up corps of pro-regime hackers, including a secretive "Cyber Army" thought to be linked to the country's powerful Revolutionary Guard. Lebanon's Iran-backed militant Hezbollah group is also believed to count skilled hackers among its ranks.

Tehran has been on the receiving end of a series of computer attacks in recent years.

Iranian technicians cut off Internet links to Iran's Oil Ministry, rigs and

the hub for nearly all the country's crude exports earlier this year as they tried to battle malicious software known as Flame, which was able to steal information and spy on users.

In 2010, a virus called Stuxnet tailored to disrupt Iran's nuclear centrifuges caused some setbacks within its uranium enrichment labs and infected an estimated 16,000 computers, Iranian officials say.

Alexander Klimburg, a computer security expert at the Austrian Institute for International Affairs, said the latest attacks against Saudi Arabia and Qatar are more complex than those typically employed by "hacktivist" groups seeking to highlight particular political or social causes.

He agrees that Iran might be involved, though he acknowledges it is difficult to know for sure.

"There has been an Iranian strategy ... to interrupt the flow of oil out of the Strait of Hormuz," he said. "Nobody's ever said they'd do it just with fast boats," a reference to the armed Revolutionary Guard craft that ply the Persian Gulf.

But other experts have their doubts.

Vitaly Kamluk, chief malware expert at Russian security company Kaspersky Lab, said that while the attacks appear to be acts of sabotage, there was no firm evidence that they were linked, nor was it known who exactly might be behind them.

"Attribution," he said, "is extremely hard in cyberspace."

Copyright 2012 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.

Citation: Virus origin in Gulf computer attacks in question (2012, September 4) retrieved 25 April 2024 from https://phys.org/news/2012-09-virus-gulf.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.