Iran: 'Flame' virus fight began with oil attack (Update)

May 30 2012, by ALI AKBAR DAREINI

In this Wednesday, Sept. 28, 2011 file photo, a part of the Maroun Petrochemical plant is seen, at the Imam Khomeini port, southwestern Iran. Technicians battling a complex computer virus took the ultimate firewall measures shutting off all Internet links to Iran's oil ministry and the terminal that carries nearly all the country's crude exports. (AP Photo/Vahid Salemi, File)

(AP) — Computer technicians battling to contain a complex virus last month resorted to the ultimate firewall measures — cutting off Internet links to Iran's Oil Ministry, rigs and the hub for nearly all the country's crude exports.

At the time, Iranian officials described it as a data-siphoning blitz on key oil networks.

On Wednesday, they gave it a name: A strike by the powerful "Flame" malware that experts this week have called a new and highly sophisticated program capable of hauling away computer files and even listening in on computer users. Its origins remain a mystery, but international suspicion quickly fell on Israel opening another front in its suspected covert wars with archenemy Tehran.

"This virus penetrated some fields. One of them was the oil sector," said Gholam Reza Jalali, who heads an Iranian military unit in charge of fighting sabotage. "Fortunately, we detected and controlled this single incident."

The Flame virus — a mix of cyberspy and hard-drive burglar — has been detected across the Middle East recently. But Iran's linkage to the oil network attack in April could mark its first major infiltration and suggests a significant escalation in attempts to disrupt Iran's key commercial and nuclear sites. Iran is one of the world's leading oil producers.

Two years ago, 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. At least two other smaller viruses have been detected in nuclear and industrial centers.

The Flame program, however, is widely considered as a technological leap in break-in programming. Some experts also see the same high level of engineering shared by Stuxnet, which many suspect was the work of Israeli intelligence.

"It is very complex and very sophisticated," said Marco Obiso, cybersecurity coordinator at the U.N.'s International Telecommunication Union in Geneva. "It's one of the most serious yet."

Israel, a world leader in computer security, has never confirmed or denied any involvement in Stuxnet or other viruses that have hit Iranian networks nationwide.

Israel fears that Iran's nuclear program is geared toward developing a weapon that might be turned against it and Israel itself is believed to have nuclear weapons.

Israeli leaders have repeatedly said that "all options are on the table," a phrase that is widely interpreted as meaning the possibility of a military strike and other measures that could include cyberwarfare.

Already, Iran and Israel have traded accusations of carrying out clandestine hits and attack conspiracies in locales stretching from the Baku to Bangkok.

Iran claims Israeli agents are behind the slayings of at least five nuclear scientists and researchers since 2010. Earlier this month, Iran hanged a man convicted of carrying out one of the killings after allegedly being trained by Israel's Mossad spy agency. Israel denied any role.

Authorities in several countries, meanwhile, are investigating possible Iranian links to bombings and plots against Israeli targets and others, including a wide-ranging probe in Azerbaijan's capital Baku.

On the cyber front, Iran says it has sharply boosted its defenses by creating special computer corps to protect crucial online infrastructure. Iran also claims it seeks to build its own Internet buffered from the global web, but experts have raised serious questions about its feasibility.

Iran's Deputy Minister of Communications and Information Technology Ali Hakim Javadi was quoted by the official IRNA news agency Wednesday as saying that Iranian experts have produced an anti-virus program capable of identifying and removing Flame.

"The anti-virus software was delivered to selected organizations in early May," he said.

That would have been at least two weeks after officials say it penetrated Iran's Oil Ministry and related sites. Within hours, technicians decided to close off the Internet connections to the ministry, oil rigs and the Khark Island oil terminal, the jump off point for about 80 percent of Iran's daily 2.2 million barrels of crude exports.

Gholam Reza Jalali, who heads an Iranian military unit in charge of fighting sabotage, told state radio that the oil industry was the only governmental body seriously affected and that all data lost were later retrieved.

"This virus penetrated some fields. One of them was the oil sector. Fortunately, we detected and controlled this single incident," Jalali said.

Obiso, whose agency is helping to direct the international response to Flame, said the virus first came to the group's attention in mid-April and researchers have been working on unraveling its code since.

"We still think Flame has much more to show," he said.

The Russian Internet security firm Kaspersky Lab ZAO said the Flame virus has struck Iran the hardest, but has been detected in the Palestinian territories, Sudan, Syria, Lebanon, Saudi Arabia and Egypt.

It also has been found in Israel — leading some Israeli security officials to suggest the virus could be traced to the U.S. or other Western nations.

Experts describe it as a multitasking mole. It can wipe data off hard drives, but also be a tireless eavesdropper by activating audio systems to listen in on Skype calls or office chatter. It also can also take screenshots, log keystrokes and — in one of its more novel functions— steal data from Bluetooth-enabled mobile phones.

Israeli's vice premier on Tuesday did little to deflect suspicion about the country's possible involvement.

"Whoever sees the Iranian threat as a significant threat is likely to take various steps, including these, to hobble it," Moshe Yaalon told Army Radio when asked about Flame. "Israel is blessed with high technology, and we boast tools that open all sorts of opportunities for us."

Iran says is has previously discovered one more espionage virus, Duqu, but that the malware did no harm Iran's nuclear or industrial sites. Jalali said Flame is the third.

Dozens of unexplained explosions also have hit the country's gas pipelines in the past two years. Officials have not linked them to cyberattacks, but authorities have not closed the books on the investigations.

Citation: Iran: 'Flame' virus fight began with oil attack (Update) (2012, May 30) retrieved 22 July 2024 from https://phys.org/news/2012-05-iran-defeated-flame-virus.html