"Flame" can sabotage computers, attack Iran: expert

Iran had previously blamed Flame for causing data loss on computers in the country's main oil export terminal and Oil Ministry. But prior to Symantec's discovery, cyber experts had only unearthed evidence that proved Flame could spy on conversations on the computers it infects and steal data.

Symantec researcher Vikram Thakur said on Thursday that the company has now identified a component of Flame that allows operators to delete files from computers, which means it can cause critical programs to fail or completely disable operating systems.

"These guys have the capability to delete everything on the computer," Thakur said. "This is not something that is theoretical. It is absolutely there."

Flame was deployed at least five years ago and is the most sophisticated cyber spying program ever discovered. Researchers have been racing to better understand its capabilities ever since Moscow-based Kaspersky Lab uncovered Flame last month after the security firm was asked by a United Nations agency to look for a virus that Iran said had sabotaged its computers, deleting valuable data.

Last week, researchers at Kaspersky Lab linked some of the software code in Flame to the Stuxnet cyber weapon, which was widely believed to have been used by the United States and Israel to attack Iran's nuclear program. Symantec later also said Stuxnet and Flame shared some code.

Current and former U.S. and Western national security officials told Reuters this week that the United States played a role in creating Flame. The Washington Post reported that U.S. and Israel jointly developed Flame and used it to collect intelligence to help slow Iran's nuclear program.

Iran complained about the threat of cyber attacks again on Thursday, saying it had detected plans by the United States, Israel and Britain to launch a "massive" strike after the breakdown of talks over Tehran's nuclear activities. It was not clear if the cyber attack referred to Flame, or a new virus.

Symantec declined to comment on who the firm believes is behind Flame.

INFRASTRUCTURE AT RISK

If Symantec's conclusions are validated, that means Flame could be used as a weapon to attack computers that run critical infrastructure systems, including dams, chemical plants and manufacturing facilities, security specialists said.

Boldizsár Bencsath, an expert on cyber warfare with Hungary's Laboratory of Cryptography and System Security, said there was at least a 70 percent chance that Flame was used to attack Iran in April.

"Of course it can be used for sabotage," said Bencsath, who began investigating Flame several weeks before it was first reported to the public. "It may have been used to attack critical infrastructure and it may be used in the future."

Sean McGurk, a former Department of Homeland Security official who helped direct the U.S. effort to protect critical infrastructure from cyber attacks, said that Flame was not the first piece of malicious software designed to sabotage systems by deleting data.

What makes it unique, he said, is that the data-wiping module works alongside a suite of other programs including the espionage tools that have previously been identified.

"It could render computing devices useless," said McGurk, who is now chief executive of a consulting firm known as NExt Generation Micro LLC.

That presents a threat, he said, because computers are used in all sorts of industrial control systems, affecting everything from critical processes at manufacturing plants to the pressure inside water networks. "Cyber elements can have catastrophic impacts," he said.

Neil Fisher, vice president for global security solutions at Unisys, said Symantec's findings - if verified - mean that Flame could be "highly dangerous."

"Many of our utilities have connected their operational management to the Internet to save costs," he said.

"Water, gas, electricity certainly constitute the critical national infrastructure," he added. "Dysfunction of those ... systems could have uncomfortable consequences for a large number of people."

(Additional reporting by William Maclean in London; Editing by Tim Dobbyn, Tiffany Wu and Bernard Orr)