

By Jim Finkle



SAN FRANCISCO (Reuters) - Researchers at Symantec Corp have uncovered a version of the Stuxnet computer virus that was used to attack Iran's nuclear program in November 2007, two years earlier than previously thought.

Stuxnet, which is widely believed to have been developed by the United States and Israel, was discovered in 2010 after it was used to attack a uranium enrichment facility at Natanz, Iran. It was the first publicly known example of a virus being used to attack industrial machinery.

Symantec researchers said on Tuesday they have uncovered a piece of code, which they called "Stuxnet 0.5," among the thousands of versions of the virus they recovered from infected machines.

They found evidence Stuxnet 0.5 was in development as early as 2005, when Iran was still setting up its uranium enrichment facility, and the virus was deployed in 2007, the same year the Natanz facility went online.

"It is really mind blowing that they were thinking about creating a project like that in 2005," Symantec researcher Liam O'Murchu told Reuters.

Security experts who reviewed Symantec's 18-page report on Stuxnet 0.5 said it showed the cyber weapon was already powerful enough to cripple output at Natanz as far back as six years ago.

"This attack could have damaged many centrifuges without destroying so many that the plant operator would have become suspicious," said a report by the Institute for Science and International Security, which is led by former United Nations weapons inspector David Albright and closely monitors Iran's nuclear program.

### ALTERNATE APPROACH

Although it is unclear what damage Stuxnet 0.5 might have caused, Symantec said it was designed to attack the Natanz facility by opening and closing valves that feed uranium hexafluoride gas into centrifuges, without the knowledge of the operators of the facility.

Previously dissected versions of Stuxnet are all believed to have been used to sabotage the enrichment process by changing the speeds of those gas-spinning centrifuges without the knowledge of their operators.

"The report provides even more concrete evidence that the United States has been activity trying to derail the Iranian nuclear program since it was restarted under President Mahmoud Ahmadinejad's reign," said John Bumgarner, an expert on cyber weapons who works as chief

technology officer with the U.S. Cyber Consequences Unit.

The Natanz facility has been the subject of intense scrutiny by the United States, Israel and allies, who charge that Iran is trying to build a nuclear bomb.

The United States began building a complex cyber weapon during the George W. Bush administration to prevent Tehran from acquiring nuclear weapons, U.S. officials familiar with the program have told Reuters. The government has declined to comment on the reports and has launched investigations into leaks on its cyber programs.

Since Stuxnet's discovery in 2010, security researchers have uncovered a handful of other sophisticated pieces of computer code they believe were developed in tandem to engage in espionage and warfare. These include Flame, Duqu and Gauss.

Stuxnet 0.5 was written using much of the same code as Flame, according to Symantec's report, which was published at the RSA security conference in San Francisco, an event attended by more than 20,000 security professionals.

Symantec said it has now uncovered four versions of Stuxnet and there are likely others that have not been discovered yet. Researchers at Symantec and elsewhere are still trying to understand the full extent of the virus's capabilities.

"This fills in some of the gaps," said O'Murchu.

He said the researchers found no evidence to prove who was behind Stuxnet.

Later versions of Stuxnet, which manipulates industrial control software known as Step 7 from Siemens AG, used more sophisticated methods to infect computer systems, he said.

Siemens previously said it plugged the security holes that allowed Stuxnet to breach its software. A company spokesman had no immediate comment on Symantec's latest research.

(Reporting By Jim Finkle in San Francisco. Additional reporting by Mark Hosenball in Washington. Editing by Andre Grenon; Editing by Tiffany Wu and Steve Orlofsky)