Stuxnet infects 30,000 industrial computers in Iran: report

September 26 2010

A general view of the reactor building at the Bushehr nuclear power plant in southern Iran in August 2010. Iranian officials said that the Stuxnet computer worm has infected 30,000 computers in Iran but has failed to "cause serious damage."

The Stuxnet computer worm has infected 30,000 computers in Iran but has failed to "cause serious damage," Iranian officials were quoted as saying on Sunday.

Some 30,000 IP addresses have been infected by Stuxnet so far in Iran, Mahmoud Liayi, head of the information technology council at the ministry of industries, was quoted as saying by the government-run paper Iran Daily.

Stuxnet, which was publicly identified in June, was tailored for Siemens

supervisory control and data acquisition (SCADA) systems commonly used to manage water supplies, oil rigs, power plants and other industrial facilities.

Stuxnet is able to recognize a specific facility's control network and then destroy it, according to German computer security researcher Ralph Langner, who has been analysing the malicious software, or malware.

Langner suspected Stuxnet's target was the Bushehr nuclear facility in Iran, where unspecified problems have been blamed for getting the facility fully operational.

Siemens, however, claims its software has not been installed at the Russian-built plant, and no Iranian official has hinted that nuclear facilities may have been infected by the malware.

"The worm has not been able to penetrate or cause serious damage to government systems," telecommunications minister Reza Taqipour was quoted as saying by the Iran Daily.

"No serious damage to industrial systems (by Stuxnet) have been reported in the country," he added.

According to the paper, another telecommunications official, Saeed Mahdiyoun, said "teams of experts had begun to systematically eliminate the virus."

"It is likely a (foreign) government project," given its complexity, Liayi added without giving further details.

Iran Daily cited various experts who suggested the United States and Israel were behind the malware, evoking the "West's electronic warfare against Iran."

An Iranian youth browses at an internet cafe in the city of Hamadan, 2009. Iranian officials said that the Stuxnet computer worm has infected 30,000 computers in Iran but has failed to "cause serious damage."

Liyai said industries were currently receiving systems to combat Stuxnet, while stressing that Iran had decided not to use anti-virus softwares developed by Siemens because "they could be carrying a new version of the malware."

"When Stuxnet is activated, the industrial automation systems start transmitting data about production lines to a main designated destination by the virus. There, the data is processed by the worm's architects and then engineer plots to attack the country," Liayi said.

The worm has been found lurking on Siemens systems mostly in India, Indonesia, Pakistan, but the heaviest infiltration appears to be in Iran, according to software security researchers.

Iran's nuclear programme is at the heart of a conflict between Tehran and the West, which suspects the Islamic republic is seeking to develop atomic weapons under the cover of a civilian drive.

Iran denies the allegation and has pressed on with its nuclear programme despite four sets of UN Security Council sanctions.

(c) 2010 AFP