September 25, 2010

Iran Fights Malware Attacking Computers

By DAVID E. SANGER

WASHINGTON — The Iranian government agency that runs the country's nuclear facilities, including those the West suspects are part of a weapons program, has reported that its engineers are trying to protect their facilities from a sophisticated computer worm that has infected industrial plants across Iran.

The agency, the Atomic Energy Organization, did not specify whether the worm had already infected any of its nuclear facilities, including Natanz, the underground enrichment site that for several years has been a main target of American and Israeli covert programs.

But the announcement raised suspicions, and new questions, about the origins and target of the worm, Stuxnet, which computer experts say is a far cry from common computer malware that has affected the Internet for years. A worm is a self-replicating malware computer program. A virus is malware that infects its target by attaching itself to programs or documents.

Stuxnet, which was first publicly identified several months ago, is aimed solely at industrial equipment made by Siemens that controls oil pipelines, electric utilities, nuclear facilities and other large industrial sites. While it is not clear that Iran was the main target — the infection has also been reported in Indonesia, Pakistan, India and elsewhere — a disproportionate number of computers inside Iran appear to have been struck, according to reports by computer security monitors.

Given the sophistication of the worm and its aim at specific industrial systems, many experts believe it is most probably the work of a state, rather than independent hackers. The worm is able to attack computers that are disconnected from the Internet, usually to protect them; in those cases an infected USB drive is plugged into a computer. The worm can then spread itself within a computer network, and possibly to other networks.

The semiofficial Mehr news agency in Iran on Saturday quoted Reza Taghipour, a top official of the Ministry of Communications and Information Technology, as saying that "the effect and damage of this spy worm in government systems is not serious" and that it had been "more or less" halted.

But another Iranian official, Mahmud Liai of the Ministry of Industry and Mines, was quoted as saying that 30,000 computers had been affected, and that the worm was "part of the electronic warfare against Iran."

ISNA, another Iranian news agency, had reported Friday that officials from Iran's atomic energy agency had been meeting in recent days to discuss how to remove the Stuxnet worm, which exploits some previously unknown weaknesses in Microsoft's Windows software. Microsoft has said in recent days that it is fixing those vulnerabilities.

It is extraordinarily difficult to trace the source of any sophisticated computer worm, and nearly impossible to determine for certain its target.

But the Iranians have reason to suspect they are high on the target list: in the past, they have found evidence of sabotage of imported equipment, notably power supplies to run the centrifuges that are used to enrich uranium at Natanz. The New York Times reported in 2009 that President George W. Bush had authorized new efforts, including some that were experimental, to undermine electrical systems, computer systems and other networks that serve Iran's nuclear program,

according to current and former American officials.

The program is among the most secret in the United States government, and it has been accelerated since President Obama took office, according to some American officials. Iran's enrichment program has run into considerable technical difficulties in the past year, but it is not clear whether that is because of the effects of sanctions against the country, poor design for its centrifuges, which it obtained from Pakistan, or sabotage.

"It is easy to look at what we know about Stuxnet and jump to the conclusion that it is of American origin and Iran is the target, but there is no proof of that," said James Lewis, a senior fellow at the Center for Strategic and International Studies in Washington and one of the country's leading experts on cyberwar intelligence. "We may not know the real answer for some time."

Based on what he knows of Stuxnet, Mr. Lewis said, the United States is "one of four or five places that could have done it — the Israelis, the British and the Americans are the prime suspects, then the French and Germans, and you can't rule out the Russians and the Chinese."

President Obama has talked extensively about developing better cyberdefenses for the United States, to protect banks, power plants, telecommunications systems and other critical infrastructure. He has said almost nothing about the other side of the cybereffort, billions of dollars spent on offensive capability, much of it based inside the National Security Agency.

The fact that the worm is aimed at Siemens equipment is telling: the company's control systems are used around the world, but have been spotted in many Iranian facilities, say officials and experts who have toured them. Those include the new Bushehr nuclear power plant, built with Russian help.

But Bushehr is considered by nuclear weapons experts to be virtually no help to Iran in its suspected weapons program; there is more concern about the low-enriched uranium produced at Natanz, which could, with a year or more of additional processing, be converted to bomb fuel.

John Markoff contributed reporting from San Francisco, and William Yong from Tehran.