Computer attacks linked to wealthy group or nation

September 26 2010, By LOLITA C. BALDOR , Associated Press Writer

(AP) -- A powerful computer code attacking industrial facilities around the world, but mainly in Iran, probably was created by experts working for a country or a well-funded private group, according to an analysis by a leading computer security company.

The malicious code, called Stuxnet, was designed to go after several "high-value targets," said Liam O Murchu, manager of security response operations at Symantec Corp. But both O Murchu and U.S. government experts say there's no proof it was developed to target nuclear plants in Iran, despite recent speculation from some researchers.

Creating the malicious code required a team of as many as five to 10 highly educated and well-funded hackers. Government experts and outside analysts say they haven't been able to determine who developed it or why.

The malware has infected as many as 45,000 computer systems around the world. Siemens AG, the company that designed the system targeted by the worm, said it has infected 15 of the industrial control plants it was apparently intended to infiltrate. It's not clear what sites were infected, but they could include water filtration, oil delivery, electrical and nuclear plants.

None of those infections has adversely affected the industrial systems, according to Siemens.

U.S. officials said last month that the Stuxnet was the first malicious computer code specifically created to take over systems that control the inner workings of industrial plants.

The Energy Department has warned that a successful attack against critical control systems "may result in catastrophic physical or property damage and loss."

Symantec's analysis of the code, O Murchu said, shows that nearly 60 percent of the computers infected with Stuxnet are in Iran. An additional 18 percent are in Indonesia. Less than 2 percent are in the U.S.

"This would not be easy for a normal group to put together," said O Murchu. He said "it was either a well-funded private entity" or it "was a government agency or state sponsored project" created by people familiar with industrial control systems.

A number of governments with sophisticated computer skills would have the ability to create such a code. They include China, Russia, Israel, Britain, Germany and the United States. But O Murchu said no clues have been found within the code to point to a country of origin.

Iran's nuclear agency has taken steps to combat the computer worm that has affected industrial sites in the country,ghout the country, including its first nuclear power station just weeks before it was set to go online. Experts from the Atomic Energy Organization of Iran met this past week to discuss how to remove the malware, according to the semiofficial ISNA news agency.

The computer worm, which can be carried or transmitted through portable thumb drives, also has affected the personal computers of staff working at the plant, according to IRNA, Iran's official news agency. The news agency said it has not caused any damage to the plants major

systems.

German security researcher Ralph Langner, who has also analyzed the code, told a computer conference in Maryland this month that his theory is that Stuxnet was created to go after the nuclear program in Iran. He acknowledged, though, that the idea is "completely speculative."

O Murchu said there are a number of other possibilities for targets, including oil pipelines. He said Symantec soon will release details of its study in the hope that industrial companies or experts will recognize the specific system configuration being targeted by the code and know what type of plant uses it.

At the Homeland Security Department's National Cybersecurity & Communications Integration Center, a top U.S. cyberofficial on Friday displayed a portable flash drive containing the Stuxnet code and said officials have been studying it in the lab.

"I've let this run wild to see what it would do," said Sean McGurk, director of the cyberoperations center. "So far we haven't seen a lot of smoke coming out, so we know it's not doing anything specifically malicious right now."

Experts at the Energy Department's Idaho National Laboratory have been analyzing it.

McGurk said that "it's very difficult to know what the code was developed for. When you talk about specifically attributing it to a facility with a set purpose from a nation-state actor or criminal actor or 'hacktivist,' it's very difficult for us to say specifically, 'This is what it was targeted to do.'"

Experts in Germany discovered the worm, and German officials

transmitted the malware to the U.S. through a secure network. The two computer servers controlling the malware were in Malaysia and Denmark, O Murchu said, but both were shut down after they were discovered by computer security experts earlier this summer.

In plain terms, the worm was able to burrow into some operating systems that included software designed by Siemens AG, by exploiting a vulnerability in several versions of Microsoft Windows.

Unlike a virus, which is created to attack computer code, a worm is designed to take over systems, such as those that open doors or turn physical processes on or off.