

Available on the iPad

Iran was prime target of SCADA worm

July 23, 2010, 8:40 PM EDT

 By Robert McMillan

Computers in Iran have been hardest hit by a dangerous computer worm that tries to steal information from industrial control systems.

According to data compiled by [Symantec](#), nearly 60 percent of all systems infected by the worm are located in Iran. Indonesia and India have also been hard-hit by the malicious software, known as Stuxnet.

Looking at the dates on digital signatures generated by the worm, the malicious software may have been in circulation since as long ago as January, said Elias Levy, senior technical director with Symantec Security Response.

Stuxnet was discovered last month by VirusBlokAda, a Belarus-based antivirus company that said it found the software on a system belonging to an Iranian customer. The worm seeks out Siemens SCADA (supervisory control and data acquisition) management systems, used in large manufacturing and utility plants, and tries to upload industrial secrets to the Internet.

Symantec isn't sure why Iran and the other countries are reporting so many infections. "The most we can say is whoever developed these particular threats was targeting companies in those geographic areas," Levy said.

The U.S. has a long-running trade embargo against Iran. "Although Iran is probably one of the countries that has the worst infections of this, they are also probably a place where they don't have much AV right now," Levy said.

Siemens wouldn't say how many customers it has in Iran, but the company now says that two German companies have been infected by the virus. A free virus scanner posted by Siemens earlier this week has been downloaded 1,500 times, a company spokesman said.

Earlier this year, Siemens said it planned to wind down its Iranian business -- a 290-employee unit that netted $\square\square\square$ 438 million (US\$562.9 million) in 2008, according to the [Wall Street Journal](#). Critics say the company's trade there has helped feed Iran's nuclear development effort.

Symantec compiled its data by working with the industry and redirecting traffic aimed at the worm's command and control servers to its own computers. Over a three-day period this week, computers located at 14,000 IP addresses tried to connect with the command and control servers, indicating that a very small number of PCs worldwide have been hit by the worm. The actual number of infected machines is probably in the 15,000 to 20,000 range, because many companies place several systems behind one IP address, according to Symantec's Levy.

Because Symantec can see the IP address used by machines that try to connect with the command and control servers, it can tell which companies have been infected. "Not surprisingly, infected machines include a variety of organizations that would use SCADA software and systems, which is clearly the target of the attackers," the company said in its blog post Thursday.

Stuxnet spreads via USB devices. When an infected USB stick is viewed on a Windows machine, the code looks for a Siemens system and copies itself to any other USB devices it can find.

A temporary workaround for the Windows bug that allows Stuxnet to spread can be found [here](#).

Robert McMillan covers computer security and general technology breaking news for The IDG News Service. Follow Robert on Twitter at [@bobmcmillan](#).

Robert's e-mail address is robert_mcmillan@idg.com

Related Articles

- Shortened URLs Drive Need for New Security - PCWorld Business Center
- Shortened URLs Drive Need for New Security
- 4 Ways to Get a White iPhone 4 Now - PCWorld
- Shortened URL spam shows big rise

Copyright IDG News Service\San Francisco Bureau