Security
May 2, 2009 9:29 AM PDT

Feds' red tape left medical devices infected with computer virus

by Stephanie Condon

The **Conficker** Internet virus has infected important computerized medical devices, but governmental red tape interfered with their repair, an organizer of an antivirus working group told Congress on Friday.

Rodney Joffe, one of the founders of an unofficial organization known as the Conficker Working Group, said that government regulations prevented hospital staff from carrying out the repairs.

Joffe, who also is the senior vice president for the telecom clearinghouse Neustar, told a panel of the House Energy and Commerce Committee that over the last three weeks, he and another **Conficker researcher identified at least 300 critical medical devices** from a single manufacturer that have been infected with the computer virus.

The devices were used in hospitals to allow doctors to view and manipulate high-intensity scans like MRIs and were often found in or near intensive care unit facilities, connected to local area networks with other critical medical devices.

"They should have never, ever been connected to the Internet," Joffe said.

Regulatory requirements mandated that the impacted hospitals would have to wait 90 days before the systems could be modified to remove the infections and vulnerabilities.

Joffe's testimony and earlier reports of infected medical devices show the risks involved in efforts to reap the economic benefits of a networked world. President

Obama's stimulus package has allocated billions of dollars for digitizing medical records and networking the nation's electric grids.

"The open Internet, one of its great values is it allows you to connect fairly cheaply and fairly easily to other computers," Joffe said. He added, however, that "the Internet was never designed to do the things it's doing today."

That includes connecting control systems to the Internet to **manipulate and coordinate the nation's electric grids**.

"The future of widespread (electric) meter-to-meter communication does have me concerned," said Dan Kaminsky, a technology consultant who last year discovered a **critical flaw in the Internet's core infrastructure**. "I would like to see more security for those meters."

It was recently reported that **Chinese and Russian spies had infiltrated the grid networks**. Politicians **introduced a bill** on Thursday to give the Homeland Security Department and other federal agencies more authority over utilities in order to protect the "smart" grid from cyberattacks.

Joffe and other witnesses said that, at an operational level, the DHS is the appropriate government agency to improve cybersecurity. He called the U.S. Computer Emergency Readiness Team, which is operated by the DHS, "woefully understaffed and woefully underfunded." As part of its mission, USCERT acts as a liaison between the public and private sectors.

Gregory Nojeim, senior counsel for the Center for Democracy and Technology, also said DHS should naturally hold jurisdiction over cybersecurity, as long as it makes its actions more transparent and receives policy guidance from the White House.

Policymakers need to be clear and open in their work with the private sector, Nojeim said, and should avoid giving anyone in the government--even the president--too much power over private networks. He urged the congressional panel to reject legislation from Senator Jay Rockefeller, D-W.Va., that would give the president power to shut down any critical network--federal or otherwise--in an emergency.

"Any such shutdown could also have far-reaching, unintended consequences for the economy and for the critical infrastructures themselves," he said. "To our knowledge, no circumstance has yet arisen that could justify a presidential order to limit or cut off Internet traffic to a particular critical infrastructure system when the operators of that system think it should not be limited or cut off."

*This story was originally published on **CBSNews.com**.*

Stephanie Condon is a staff writer for CBSNews.com focused on the intersection of technology and politics. She is based in Washington, D.C. E-mail Stephanie.

Topics: **Vulnerabilities & attacks**

Tags: **Conficker**, **network security**, **hospitals**, **e-health**

Related

From CNET

Prediction: Apple will recommend security software

Hunt for a Windows laptop...on a Mac?

McAfee: New botnets dwarf Conficker threat

From around the web

Gadgetwise: Mac Security Part II: It's a... The New York Times

Hotels: Hyatt is the latest chain on sal... Budget Travel