Security
April 23, 2009 4:23 PM PDT

Conficker infected critical hospital equipment, expert says

by Elinor Mills

Updated 7:50 a.m. PDT April 24 to specify that the infection was in the U.S.

SAN FRANCISCO--The Conficker worm infected several hundred machines and critical medical equipment in an undisclosed number of U.S. hospitals recently, a security expert said on Thursday in a panel at the RSA security conference.

"It was not widespread, but it raises the awareness of what we would do if there were millions" of computers infected at hospitals or in critical infrastructure locations, Marcus Sachs told CNET News after the session. Sachs is the director of the SANS Internet Storm Center and a former White House cybersecurity official.

It is unclear how the devices, which control things like heart monitors and MRI machines, and the PCs got infected, he said. The computers are older machines running Windows NT and Windows 2000 in a local area network that was not supposed to have access to the Internet, however, the network was connected to one that has direct Internet access and so they were infected, he said.

Conficker spreads via networked computers as well as through removable storage devices and a hole in Windows that Microsoft patched in October, but these machines were too old to be patched, according to Sachs.

In the U.K., PCs at hospitals in Sheffield were found to be infected with Conficker in January, **The Register reported**.

The situation illustrates the dangers of connecting critical networks, like in hospitals

and in SCADA (Supervisory Control and Data Acquisition) systems used by utilities and other critical infrastructure providers, with networks connected to the Internet, he said during the panel "Securing Critical Infrastructures: Infrastructure Exposed."

"We haven't found any nukes yet that are infected with Conficker or that are trying things like Twitter," he quipped. But "that is within the probable as we take shortcuts," he said.

"We're seeing a huge uptick in probing for SCADA systems," said Jerry Dixon, director of analysis and vice president of government relations at research firm Team Cymru. For years, the SCADA systems were separated from the public networks, but that's not the case anymore, he said.

Utilities move to remote access and other Internet-based technologies so workers can have access to the control systems when they are not at the plant and to cut costs, Sachs said. Workers have been known to access control systems using BlackBerrys for no reason other than that they can, he said.

Asked after the panel if cyberattacks had led to any utility outages, Michael Assante, chief security officer of the North American Electrical Reliability Corporation (NERC), said "none in North America."

"There is no evidence of computer compromise that led to a disruption of service," he said. "We're not immune to it; it's not hypothetical."

Government officials maintained that an electricity blackout in 2003 in the northeastern United States was not caused by the Blaster Internet worm that was circulating at the time as was suspected, but officials also were never able to reveal why it happened.

Elinor Mills covers Internet security and privacy. She joined CNET News in 2005 after working as a foreign correspondent for Reuters in Portugal and writing for The Industry Standard, the IDG News Service, and the Associated Press. E-mail Elinor.

Topics: **Vulnerabilities & attacks**

Tags: **Conficker**, **critical infrastructure**, **hospitals**

Share: Digg Del.icio.us Reddit Yahoo! Buzz Facebook

Related

From CNET

Gates: Cyberattacks a constant threat

Windows 7 security enhancements

Researchers say Conficker is all about the money

From around the web

Conficker Removal Reminders Washington Post Blogs - Faster...

Conficker's April Fools Fizzled, But Thr... Washington Post Blogs - Securi...

More related posts powered by Sphere