Conficker worm hits hospital devices

April 30 2009, By Elise Ackerman

A computer worm that has alarmed security experts around the world has crawled into hundreds of medical devices at dozens of hospitals in the United States and other countries, according to technologists monitoring the threat.

The worm, known as "Conficker," has not harmed any patients, they say, but it poses a potential threat to hospital operations.

"A few weeks ago, we discovered medical devices, MRI machines, infected with Conficker," said Marcus Sachs, director of the Internet Storm Center, an early warning system for Internet threats that is operated by the SANS Institute.

Around March 24, researchers monitoring the worm noticed that an imaging machine used to review high-resolution images was reaching out over the Internet to get instructions -- presumably from the programmers who created Conficker.

The researchers dug deeper and discovered that more than 300 similar devices at hospitals around the world had been compromised. The manufacturer of the devices told them none of the machines were supposed to be connected to the Internet _ and yet they were. And because the machines were running an unpatched version of Microsoft's operating system used in embedded devices they were vulnerable.

Normally, the solution would be simply to install a patch, which Microsoft released in October. But the device manufacturer said rules

from the U.S. Food and Drug Administration required that a 90-day notice be given before the machines could be patched.

"For 90 days these infected machines could easily be used in an attack, including, for example, the leaking of patient information," said Rodney Joffe, a senior vice president at NeuStar, a communications company that belongs to an industry working group created to deal with the worm. "They also could be used in an attack that affects other devices on the same networks."

Joffe, who is scheduled to testify before Congress on Friday, said he will ask lawmakers to remove the barriers to coordination between federal agencies so that cyberthreats like Conficker can be addressed.

In addition to the medical-imaging machines, Joffe said the working group has seen thousands of other machines located in hospitals reach out to the Conficker mastermind by contacting another computer on the Internet for instructions. Researchers have not determined the function of these machines. They could be a personal computer sitting on a secretary's desk or more sensitive medical devices linked to patient care.

"Hopefully, the malware writers didn't have a lot of insight into how these medical devices work," said Patrik Runald, chief security adviser for F-Secure, a computer-security company based in Finland. Runald said the worm had also been found at a hospital in Sweden and several hospitals in England earlier this year.

And the danger isn't contained to hospitals.

"Microsoft Windows is a common operating system for embedded devices that is used in all industries," Joffe said. "There is no reason to believe that other industries don't have the same problem."

At the peak of the worm's infection in early spring, the Conficker Working Group estimated there were more than 10 million devices infected worldwide. Runald, whose company is part of the Conficker Working Group, said about 3 million devices are currently compromised as the others were cleaned up. But while experts have patched infected machines, they have not been able to stop the spread of the worm.

Conficker spreads by copying itself onto machines running Microsoft's Windows operating system that lack the security patch from October. Conficker installs itself and periodically reaches out for directions from its maker that cause it to rewrite its code, increasing its capabilities for malicious action and decreasing its chance of detection.

Joffe said he doubted that whoever made Conficker was specifically targeting medical devices or parts of the country's critical infrastructure, but that doesn't reduce the risk that key industries could be crippled by the worm.

"Once they work out what they've got, who knows who they will sell access to," he said. "This has to be fixed."

___