

The Washington Post

Hackers Have Attacked Foreign Utilities, CIA Analyst Says

By Ellen Nakashima and Steven Mufson

Washington Post Staff Writers and Washington Post Staff Writers

Saturday, January 19, 2008; A04

In a rare public warning to the power and utility industry, a CIA analyst this week said cyber attackers have hacked into the computer systems of utility companies outside the United States and made demands, in at least one case causing a power outage that affected multiple cities.

"We do not know who executed these attacks or why, but all involved intrusions through the Internet," Tom Donahue, the CIA's top cybersecurity analyst, said Wednesday at a trade conference in New Orleans.

Donahue's comments were "designed to highlight to the audience the challenges posed by potential cyber intrusions," CIA spokesman George Little said. The audience was made up of 300 U.S. and international security officials from the government and from electric, water, oil and gas companies, including BP, Chevron and the Southern Co.

"We suspect, but cannot confirm, that some of the attackers had the benefit of inside knowledge," Donahue said. He did not specify where or when the attacks took place, their duration or the amount of money demanded. Little said the agency would not comment further.

The remarks come as cyber attackers have made increasingly sophisticated intrusions into corporate computer systems, costing companies worldwide more than \$20 billion each year, according to some estimates.

Cyber extortion is a growing threat in the United States, and attackers have radically increased their take from online gambling sites, e-commerce sites and banks, which pay the money to prevent sites from being shut down and to keep the public from knowing their sites have been penetrated, said Alan Paller, research director at the SANS Institute, the cybersecurity education group that sponsored the meeting.

"The CIA wouldn't have changed its policy on disclosure if it wasn't important," Paller said. "Donahue wouldn't have said it publicly if he didn't think the threat was very large and that companies needed to fix things right now."

Over the past year to 18 months, there has been "a huge increase in focused attacks on our national infrastructure networks, . . . and they have been coming from outside the United States," said Ralph Logan, principal of the Logan Group, a cybersecurity firm.

It is difficult to track the sources of such attacks, because they are usually made by people who have disguised themselves by worming into three or four other computer networks, Logan said. He said he thinks the attacks were launched from computers belonging to foreign governments or militaries, not terrorist groups.

Over the past 10 years, electric utilities, pipelines, railroads and oil companies have used remotely controlled and monitored valves, switches and other mechanisms. This has resulted in substantial savings in man power and other costs.

But to do that, the companies have installed wireless Internet connections to link the devices to central offices.

"In the past, if they wanted to go out and read a gauge on a gas well, for example, they would have to send a technician in his vehicle; he would drive 100 miles and physically read the gauge and get back in his truck," Logan said. "Now they can read it from headquarters. But it allows attackers a gateway into the system."

In addition, within the companies' main offices, control equipment can be accessed from more computers than in the past.

The electric utility industry has also been adding software that allows more coordination among different parts of the electricity grid and will ultimately allow utilities and individuals to control devices remotely. This is a central part of what many firms call the "utility of the future," which will be better able to save energy and reduce greenhouse gas emissions.

"Often there are authentication methods that are less than secure," Logan said. "Sometimes there are no authentication methods."

On Thursday, the Federal Energy Regulatory Commission approved eight cybersecurity standards for electric utilities. They involve identity controls, training, security "perimeters," physical security of critical cyber equipment, incident reporting and recovery.

The U.S. electricity grid has always been vulnerable to outages. "Cybersecurity is a different kind of threat, however," Joseph T. Kelliher, the commission's chairman, said in a statement this week. "This threat is a conscious threat posed by a single hacker, or even an organized group that may be deliberately trying to disrupt the grid."

[View all comments](#) that have been posted about this article.

© 2009 The Washington Post Company