

» [Print](#)

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to colleagues, clients or customers, use the Reprints tool at the top of any article or visit: www.reutersreprints.com.

U.S. probes cyber attack on water system

Fri, Nov 18 2011

By [Jim Finkle](#)

(Reuters) - Federal investigators are looking into a report that hackers managed to remotely shut down a utility's water pump in central Illinois last week, in what could be the first known foreign cyber attack on a U.S. industrial system.

The November 8 incident was described in a one-page report from the Illinois Statewide Terrorism and Intelligence Center, according to Joe Weiss, a prominent expert on protecting infrastructure from cyber attacks.

The attackers obtained access to the network of a water utility in a rural community west of the state capital Springfield with credentials stolen from a company that makes software used to control industrial systems, according to the account obtained by Weiss. It did not explain the motive of the attackers.

He said that the same group may have attacked other industrial targets or be planning strikes using credentials stolen from the same software maker.

The U.S. Department of Homeland Security and the Federal Bureau of Investigation are examining the matter, said DHS spokesman Peter Boogaard.

"At this time there is no credible corroborated data that indicates a risk to critical infrastructure entities or a threat to public safety," he said, declining to elaborate further. An FBI spokesman in Illinois did not return phone calls seeking comment.

SCADA SECURITY

Cyber security experts said that the reported attack highlights the risk that attackers can break into what is known as Supervisory Control and Data Acquisition (SCADA) systems. They are highly specialized computer systems that control critical infrastructure -- from water treatment facilities, chemicals plants and nuclear reactors to gas pipelines, dams and switches on train lines.

The issue of securing SCADA systems from cyber attacks made international headlines last year after the mysterious Stuxnet virus attacked a centrifuge at a uranium enrichment facility in Iran. Many experts say that was a major setback for Iran's nuclear weapon's program and attribute the attack to the United States and Israel.

In 2007, researchers at the U.S. government's Idaho National Laboratories identified a vulnerability in the electric grid, demonstrating how much damage a cyber attack could inflict on a large diesel generator. (To see video that was leaked to CNN: [here](#))

Lani Kass, a former senior cyber policy adviser to the U.S. Joint Chiefs of Staff and the U.S. Air Force said that one day a real-life cyber attack on a U.S. SCADA system could lead to a major disaster.

"Many (SCADA systems) are old and vulnerable," said Kass. "There are no financial incentives for the utility owners to replace and secure these systems and the costs would be high."

U.S. Rep Jim Lanvein, a Democrat from Rhode Island, said that the report of the attack highlighted the need to pass legislation to improve cyber security of the U.S. critical infrastructure.

"The stakes are too high for us to fail, and our citizens will be the ones to suffer the consequences of our inaction," he said in a statement.

ILLINOIS ATTACK

Several media reports identified the location of the attack as Springfield. City officials said that was inaccurate.

Don Craven, a lawyer and a trustee for the Curran-Gardner Township Public Water District, said late on Friday that the small water utility was aware that "something happened" but that he did not have much information on the matter.

"We are aware there may have been a successful or unsuccessful attempt to hack into the system," Craven said by telephone from his Springfield, Illinois, office.

"It came through a software system that's used to remotely access the pumps," he said. "A pump is burned out."

The district serves some 2,200 customers in a rural district West of Springfield. He said there was no interruption in service as the utility operates multiple pumps and wells. Its water comes from an aquifer underneath the Sangamon River.

Craven said he did not know what software at the utility was involved but said he was confident that no customer records were compromised.

Craven said he was mystified as to the reason hackers might have targeted the tiny district.

"Maybe it's the quality of our water, which is better than Springfield's," Craven joked.

The general manager of the utility has not returned messages.

OTHER ATTACKS?

Quoting from the one-page report, Weiss said it was not yet clear whether other networks had been hacked as a result of the breach at the U.S. software maker.

He said the manufacturer of that software keeps login credentials to the networks of its customers so that its staff can help them support those systems.

"An information technology services and computer repair company checked the computer logs of the system and determined the computer had been hacked into from a computer located in Russia," Weiss quoting from the report in a telephone interview with Reuters.

Workers at the targeted utility in central Illinois on November 8 noticed problems with SCADA systems which manages the water supply system, and discovered that a water pump had been damaged, said Weiss, managing partner of Applied Control Solutions in Cupertino, California.

(Reporting by Jim Finkle in Boston; Additional reporting by [Jim Wolf](#), [Andrew Stern](#), [Diane Bartz](#) and [Andrea Shalal-Esa](#); Editing by Steve Orlofsky, [Bernard Orr](#))

© Thomson Reuters 2011. All rights reserved. Users may download and print extracts of content from this website for their own personal and non-commercial use only. Republication or redistribution of Thomson Reuters content, including by framing or similar means, is expressly prohibited without the prior written consent of Thomson Reuters. Thomson Reuters and its logo are registered trademarks or trademarks of the Thomson Reuters group of companies around the world.

Thomson Reuters journalists are subject to an Editorial Handbook which requires fair presentation and disclosure of relevant interests.

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to colleagues, clients or customers, use the Reprints tool at the top of any article or visit: www.reutersreprints.com.