Pennsylvania Water Hack Brings Total to Ten

According to a number of media sources, the FBI is investigating a computer security breach at the Harrisburg, PA water treatment facility. A foreign-based hacker operating over the Internet tapped into an employee's laptop and then used an employee's remote access as the point of entry into the SCADA system. The hacker then installed a malware and spyware in the water plant computer system, officials said. An FBI special agent says the attackers were apparently not targeting the plant, but intended "to use the computer as a resource for distributing e-mails of whatever electronic information they had planned." News reports on the event can be found at:

http://www.computerworld.com
http://www.washingtontimes.com

The Industrial Security Incident Database records this as its seventh incident, including several similar events where poor separation between SCADA systems and business systems in the water industry allowed keyloggers and spyware to be installed on critical HMI computers. Virus infiltration has also been a leading cause of incidents for the water industry.

The Columbus Day weekend intrusion is the fourth WaterISAC recorded cyber-attack on a U.S. water supply in the past four years, but ISID records show a number of other events (WaterISAC is an industry information sharing and analysis center with members from among more than 1,000 drinking water and wastewater systems in the U.S). In one of three past attacks cited by WaterISAC, hackers used a Korea-based telecom to launch a denial of service attack on one water supply. In a second, they penetrated a top-level data control and acquisition system on a California irrigation district wastewater treatment plant. And in a third, they announced their entry into the computer system with a message, "I enter in your server like you in Iraq." Combined with the ISID total, it appears that the confirmed total number of incidents in the water industry is now up to ten. Until the last few years the water industry did not seem to be experiencing the same rate of incidents as other industries. This difference has appeared to disappear as the industry upgrades its SCADA networks to Ethernet and TCP/IP based systems.