WaterISAC
Water Security Network

MEMORANDUM

Date: April 10, 2013

To: Charles Hilton, WSCC Chair

Cc: John Sullivan, WaterISAC Chair

From: WaterISAC

Subject: Recent Reported Water Sector Cyber Events

November 2011 – an alleged intrusion from a Russian IP address resulted in physical damage to a pump at a water utility in Springfield, Illinois. Further investigation determined this was a third party contractor employed by the utility accessing the network while on a trip to Russia. Damage to the pump was unrelated. Although this turned out to not be an actual incident, it highlights potential vulnerabilities that exist with remote access and connectivity of control system devices to the Internet.

November 2011 – in response to the events in Springfield, a hacker accessed and took screen shots of a SCADA system at a utility in South Houston, Texas. He later shared the screen shots on a popular website for hackers to identify their activities and disclose stolen data. The intrusion did not cause any damage, and the individual responsible claimed he did this to demonstrate how easy it was to do so. Once again, the incident highlights the potential threat posed by connectivity to the internet.

August 2012 – a number of utilities received a suspicious email claiming to be a security researcher in Iran. In coordination with ICS-CERT, it was determined that this email was also received by utilities in the electric sector. It was considered a spear phishing attempt, but further analysis of any associated malware was not possible.

September 2012 – a brute force attack[1] against a remote desktop connection at a utility in Arizona was reported to WaterISAC. The utility was able to detect the anomalous activity and through its third party contractor implement additional security protocols. There is no indication the intrusion was successful.

February 2013 – JEA, the electric and water utility for the City of Jacksonville, Florida, notified its customers that its website and automatic phone system suffered a distributed denial-of-service

[1] Brute Force Attack: A hacker, or hackers, attempts to gain access to a computer, network, database asset with an application that uses trial-and-error to exhaustively explore all possible secret passwords, encryption keys, database lookup keys, etc. to unlock the asset.

(DDoS)[2] attack. The attack, which began on February 17 and lasted 3 days, impacted a limited number of payment transactions. However, there was no penetration of the JEA internal networks, customer information was not vulnerable, and there was no impact to operations at their power, water or sewer plants. This incident demonstrates there are cyber threats, beyond those targeting control systems, that have the potential to impact an organization and its customers.

March 2013 – through its local fusion center, a water system in Texas reported a DDoS attack against its business network. WaterISAC is working with government partners to obtain more details.

Internet-Facing Control System Devices

In 2011, ICS-CERT contacted 78 water utilities that were identified as having Internet-facing control system devices with a known remote access vulnerability. ICS-CERT coordinated with the vendor and provided affected utilities with guidance on best practices and mitigation strategies. In early 2013, WaterISAC assisted ICS-CERT in contacting utilities following further identification of Internet-facing control system devices as part of a project by independent researchers dubbed 'Project Shine'.

While these 'incidents' should not be ignored, as the identification of Internet-facing control system devices is becoming an increasingly popular pursuit among researchers and hackers and there are clear risks that can result from such configuration, there is no evidence that any of these devices were successfully exploited.

Eric Meyers
Lead Analyst, WaterISAC
Office: 202-331-0479
24-Hour: 866-h2o-isac x3 (866-426-4722 x3)
analyst@waterisac.org

[2] DDoS Attack: A hacker, or hackers, typically by illicitly commandeering computers infected by malware, saturate a targeted network or system with so many communications requests that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable.