Water Sector Cybersecurity Incident Case Study

#004: Ransomware – 2022
SCADA, Brief Impact but Quick Recovery with Standby SCADA Computer

INCIDENT OVERVIEW

A small-size water utility experienced a ransomware incident that briefly impacted SCADA operations.

DESCRIPTION

At 2:00 AM on a Monday, ransomware software encrypted the utility's SCADA computer. The ransomware disabled McAfee security software and encrypted the duplicated data in the Shadow Copies. The computer was relatively new and was running Windows 10. It was on a separate network from the IT network. The computer had remote access through Team Viewer as well as two older legacy instances of VNC. The attacker took advantage of VNC to get into the system. No ransom was paid.

IMPACT

The water system is dependent on SCADA for part of its operation. The ransomware encryption disabled their one live SCADA PC and threatened to disrupt service. Fortunately, as part of a recent SCADA system upgrade, the utility manager suggested that the integrator create a cold standby SCADA PC. This PC was activated in short order during the incident and normal operation was maintained. The utility did lose some regulatory reporting data. There were no significant costs incurred.

Water Sector Cybersecurity Incident Case Study

#004: Ransomware – 2022
SCADA, Brief Impact but Quick Recovery with Standby SCADA Computer - CONT'D

RESPONSE

Early on the utility manager used CISA's website to report the incident. When the ransomware situation was recognized, the utility took the compromised SCADA computer offline, and the integrator activated the cold standby SCADA computer. Initially, the method of compromise was unknown, so a risk was taken that the activated cold standby computer would have the same vulnerability and face the threat of repeat encryption. By the second day of the incident, it became clear that the compromise was achieved through the VNC connection. This remote access software was not installed on the cold standby SCADA computer. VNC was only installed on the impacted computer as a precaution in case the new approach, using Team Viewer, had any issues and they needed to fall back to the prior method. The utility planned to install WIN-911 to be alerted to future system problems.

LESSONS LEARNED

There were several valuable lessons learned from this incident, including:

- Consider maintaining cold or warm standby SCADA computers.
- Keep a written set of instructions on how to activate a standby computer in case the original system integrator is not available to assist.
- Promptly remove any just-in-case legacy remote access software once a new system has been tested.
- Keep the IT and OT networks separated.
- Establish at least a basic cybersecurity incident response plan that identifies who to contact in case of an emergency.