Water Sector Cybersecurity Incident Case Study

#003: Ransomware – 2021

SCADA, Switched to Manual and Increased Operator Rounds

INCIDENT OVERVIEW

A small-size water and wastewater utility experienced a limited ransomware incident that impacted a sewer system SCADA HMI computer, but not operations.

DESCRIPTION

On Sunday, the sewer system operator made a rounds check and found the HMI computer in an unusual state with a blue screen and a request for a password. He entered the password, and everything seemed to work normally. The following day, Monday, the operator found the same display on the HMI computer and entered the password. The screen then changed color and all the desktop icons had a "?" on them. The display asked for a bitcoin payment to release the locked files. Following directions from senior staff, the operator unplugged the computer from the power outlet and the sewer system was run manually from local control. No ransom was paid.

TECHNICAL DESCRIPTION

Based on an FBI forensics analysis of the hard drive image, on Saturday, a ransomware actor created a user account called "Support" and accessed the Windows 7 HMI computer through a Remote Desktop Protocol (RDP) connection to the "Support" account from IP address 45.77.147.22. Utility staff used a separate remote access application for operations, not RDP, which may have been left open by a vendor during the initial setup. Shortly after the RDP connection, based on a prefetch file creation, Netscan.exe appears to have been executed. The next day the computer was again accessed through RDP to the "Support" account, but this time from IP address 23.227.202.192. Two files were created, Z1.exe and Z3.exe. Mimikatz.exe appears to have been executed, followed by Z1.exe and Z2.exe. Then the files yd0N5k3r1TF75n3.exe and ai5yg89o42J4k7e.exe were created along with "HOW TO DECRYPT FILES.TXT". On Monday, it appears that the file yd0N5k3r1TF75n3.exe was executed. It was concluded that the ransomware variant used was ZuCaNo. The ransom request, which was not paid, was for 0.03 bitcoin. There was not adequate evidence to understand how the computer was originally compromised, although the assumption is through remote access from the Internet.

Water Sector Cybersecurity Incident Case Study

#003: Ransomware – 2021

SCADA, Switched to Manual and Increased Operator Rounds - CONT'D

IMPACT

There was no impact to the operation of the sewer system, as it was designed to run either manually using local control or under centralized SCADA control. However, the ransomware-encrypted SCADA computer was the main source of alarm reporting. Therefore, additional operator rounds were required to make sure everything was running properly. It was approximately three months before the computer was upgraded, integrated into the SCADA system, and resumed providing alarms, system monitoring, and control. There were no significant unexpected costs incurred as the infected computer was already scheduled for an upgrade.

RESPONSE

When faced with the locked-up SCADA HMI computer, the operator contacted the system Superintendent, who advised unplugging the computer. The Superintendent promptly contacted the state's department of environmental protection, the state's emergency management agency, their contract IT person, and notified other regional sewer operators of the situation. The FBI reached out to the utility and requested access to the computer's hard drive for forensics. The utility accommodated the request and received the hard drive back when the investigation was done. Staff seamlessly shifted to manual sewer system operation without a problem as described above.

Water Sector Cybersecurity Incident Case Study

#003: Ransomware – 2021

SCADA, Switched to Manual and Increased Operator Rounds - CONT'D

LESSONS LEARNED

Several valuable lessons were learned from this incident, including:

- Use strong and individual passwords.
- Do not leave unused RDP service ports open
- Largely isolated computers kept the ransomware from impacting additional systems.
- If a computer has been infected with ransomware, disconnect the network cable rather than the power cable to preserve additional forensics information.
- Share incident information with your fellow utilities.
- Train operators on cyber incident response, including recognizing potential problems and taking pictures of unusual computer screen displays with their phones.
- Ransomware, as in this case, is often deployed over long weekends.
- Be prepared to work with your state department of environmental protection to keep them current with the incident and any threats to service.
- Harden your remote access. The utility moved to a more secure SCADA remote access method. Everyone has their own account and password.
- Having manual system operation options is essential for uninterrupted service if your SCADA system is taken out.
- Keep your computer operating system up to date.