PACKETVIPER™

Cyber Defense of Unmanaged OT Water Assets Against a Physical Connection Breach

Case Study

Overview

Water authorities have essential, distributed operational technology (OT) network assets such as plants, pump and lift stations that increase their attack surface and present attractive targets for attackers. Connected OT assets create new attack vectors that can lead to greater exposure to cyber-threats. Unmanaged assets can be hard to get to quickly depending on the time of day, day of the week, and/or location which allows the attacker added time on the network to do damage.

In this case study, a water authority addresses challenges pertaining to the cyber-physical defense of unmanaged, digitally connected conveyance system assets. Our client executed a red team exercise to evaluate whether the PacketViper OT360 solution for remote assets (OTR) can hold up to real-world, cyber-physical attacks initiated through a physical connection at a remote OT site. The result was a success with the solution protecting the critical operations network, blocking the attacker's ability to further penetrate the network while alerting operators of the attack.

Account Profile

A Southeastern US municipal water authority with a fairly common networking environment. The OT network is flat and breaching any one location would provide open access to the network. Multiple methods of connectivity with distributed assets include cellular, fiber, and microwave radios. Many of the unmanaged OT assets are exposed with simple fencing and locks as physical protection. This city serves 6,000 residential customers with a primary water treatment plant and roughly two-dozen connected conveyance system assets spread over 200 square miles.

The Cybersecurity Challenge

Protecting unmanaged, essential distributed water assets is challenging. This is compounded based on asset location and the time it takes to 'roll a truck'. Threat vectors of concern not only include digital hackers but also "known good" vendors and system integrators who oftentimes connect to the network for normal and customary maintenance and monitoring. These physical connection threats are addressed in this exercise.

Attack Summary

These Red Team exercises simulated a physical breach whereby the team gained access to the network via a physical connection at a control panel at two of the unmanaged locations. At the first location, an IP address was obtained and the attacker attempted to identify other devices on the flat network and gain access to additional resources using an IP scanning tool. At the second location, the attacker silently connected to the network and passively listened to identify other devices and gain access to additional resources. In both cases, the Red Team activities also included attempted access to internal web-based portals and other network devices and/or PLCs.

Solution

PacketViper's agentless OTR was deployed with a ruggedized appliance and configured inline as an undetectable bridge at three unmanaged locations. Centralized management of the remote assets was set up on the unit at the water treatment plant. Sensors and proprietary, deceptive, threat detection tools were created to detect anomalies outside of normal traffic conditions such as expected PLC/HMI communications. Anomalies would then trigger the solution to automatically create a blocking rule and issue an alert.

Solution Requirements:

- The attacker will fail to identify and access the network and operators will be alerted
- Automated containment of threats inserted onto the network
- Automatic, real-time synchronization of blocking rules written upon detecting anomalous behavior
- Maintain secured 2-way communications with the OT assets

Outcome

The outcome was a success. Once on the network, the Red Team was not able to gain scanning visibility into the rest of the network. The threat in both cases was unable to move within the network due to an automated containment response directed by the solution, without orchestration with any other technology. Furthermore, an alert was sent to the operators notifying them of the anomalous behavior within the network. Upon detecting the threat, the blocking rule was pushed to all of the locations involved to ensure the threat was contained.

About PacketViper

PacketViper provides transformative and trusted cybersecurity solutions for organizations seeking to modernize the cybersecurity of converging OT and IT networks. PacketViper customers cover multiple public and private sector industries. For more visit packetviper.com.