SensorFu
ALWAYS KNOW IF YOUR NETWORK LEAKS

Protecting water utility against nation state cyber adversary

In this whitepaper we discuss:

- **Why critical infrastructure must be protected from cyber threats?**
- **What is Locked Shields?**
- **How SensorFu Beacon protected water treatment plant?**

Water supply professionals and government planners have long been aware that urban water systems are a lucrative target for cyber adversaries. Water utilities are heavily using industrial control system (ICS) networks to control the physical processes essential to water treatment and distribution systems. Network isolation and segmentation are key protections that prevent unauthorized access to these SCADA/ICS systems and to keep hostile adversaries at bay.

Locked Shields is a unique international cyber defence exercise offering the most complex technical live-fire challenge in the world. In 2019, a water treatment facility was part of targeted critical infrastructure. This article describes how SensorFu Beacon, a continuous network leak detection solution, was successfully used by a defending blue team to continuously maintain isolation of water utilities SCADA/ICS network while facing skilled and motivated adversary.

Locked Shields scenario overview

Scenario of Locked Shields 2019 exercise as described by the organizer NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE)[1] is:

> *The participating Blue Teams play the role of national rapid reaction teams (RRT) that are deployed to assist a fictional country in handling a large-scale cyber incidents and all their multiple implications. In addition to maintaining around 4000 virtualized systems while experiencing more than 2500 attacks, the teams must be effective in reporting incidents, executing strategic decisions and solving forensic, legal and media challenges. To keep up with technology developments, Locked Shields focuses on realistic scenarios and cutting-edge technologies, relevant networks and attack methods.*
>
> *According to the scenario, a fictional country, Berylia, was experiencing a deteriorating security situation, where a number of hostile events coincide with coordinated cyber attacks against a major civilian internet service provider and maritime surveillance system. The attacks caused severe*

[1] https://ccdcoe.org/exercises/locked-shields/

> *disruptions in the power generation and distribution, 4G communication systems, maritime surveillance, water purification plants and other critical infrastructure components. While the aim of the tech game was to maintain the operation of various systems under intense pressure, the strategic part addresses the capability to understand the impact of decisions made at the strategic and policy level.*

Water utility was considered as a critical capability for Berylia. Disruptions in water distribution, including water contamination, and unavailability would provide political and strategic advantage for adversary and cause significant harm to Berylian citizens and to other nation wide operations.

To protect water treatment facility, one of the blue teams in charge of cyber-defense followed best practises in implementing and operating ICS network. In particular, this blue team focused on three parts of a control system that they wanted to secure:

1. Network communications
2. Base operating systems of each host and ICS system
3. Control System applications themselves

Based on industry best practices[2] and on-site analysis blue team utilized five methods of closing identified weaknesses or mitigating their impact:

1. Blocking or limiting access to resources and services
2. Detecting malicious activity
3. Mitigating impact of possible attacks
4. Fixing core problems via e.g. operating system patches and updates.
5. Defining and implementing security policies.

Blue team based their defensive strategy on intelligence sources that they were facing cyber terrorists or nation-state adversaries with focus on the critical infrastructure of Berylia. Based on the aforementioned guidelines they implemented a layered defensive posture built around the assets in a manner that should block all but most sophisticated adversaries to gain access to assumed objectives (data munging, integrity alteration, data destruction, system destruction). Ultimately blue team based their defensive strategy on the realisation that capabilities of the attacker are not bound by their imagination nor are they infallible in building defensive measures as intended[3].

[2] https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
https://ics-cert.us-cert.gov/Recommended-Practices

SensorFu

ALWAYS KNOW IF YOUR NETWORK LEAKS

Network topology at the water utility

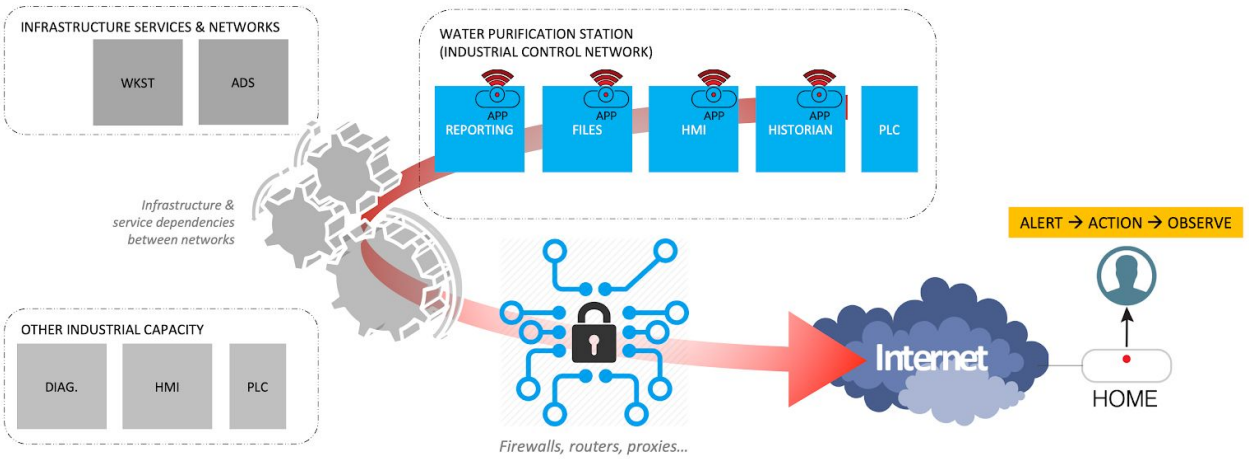

Image #1 - Network topology and SensorFu Beacon at water utility

One of the goals of Locked Shields exercises is to evaluate cutting-edge technologies and their effectiveness in life-like cyber-war. SensorFu network leak detection solution was one of the technologies that got their trial by fire in this years exercise.

SensorFu Beacon is a software product that detects new network leak paths from isolated networks or network segments. These leak paths can be a result of human error or malice, and they may violate your security policies or contractual obligations. Product consists of two parts: Beacons that continuously look for new network leak paths by the means of active network-fu, and Home that listens for successful escapes and is used to create and manage Beacons.

Beacons were deployed to isolated portions of water utility ICS network on critical servers. These assets were crucial for securing sound water purification process. Beacons provide a capability to detect network reachability changes that may occur unintentionally or intentionally on either host based network security configurations or within larger network scope.

How SensorFu Beacon saved the day

During the course of exercise it became necessary to install patches and updates to the various hosts in water utility's office network and in the ICS environment. One of the devices updated was a firewall that controlled access to and from ICS network. During the update, the team also had to update rules on the firewall. Although updated rule set was implemented using utmost care, a mistake slipped in that allowed TCP over IPv6 to be routed to and from isolated ICS network.

Accidental and unintentional opening up of IPv6 connectivity to ICS network could have allowed reaching some of the systems not designed or intended to be exposed to unauthorized access. Furthermore it would have opened a command and control channel directly to the heart of ICS network to activate and control malware that might have been already in place.

Within minutes of deploying flawed rule set, SensorFu beacon as part of it's continuous verification cycle was able to:

- Detect a leak in the water purification segment related to network isolation, more specifically IPv6 firewall rules
- Alert appropriate staff in defending blue team
- Provide actionable information to the Blue-team and IT-staff to isolate the problem and take corrective action
- Provide evidence that corrective (updated firewall ruleset) action was successful and that a leak got plugged

Rapid reaction team (RRT) was provided with timely and actionable intel from SensorFu Beacon that allowed them to block and restrict adversary movement and mitigate command and control (C2) activities needed to carry out to execute actions in attackers objectives.

During after action debriefing SensorFu's CEO Mikko Kenttälä noted:

> "Let us remember that we are really talking here a bunch of seasoned professionals who work with network and IT security on a daily basis; yet simple mistakes happen all the time. This mistake could've had catastrophic consequences - in our fictitious setting. What's scary is that this could well have been for real."

Statistics from a variety of industry reports[4] indicate that time from breach to discovery is often weeks if not longer. Therefore pro-active and easy to deploy technologies that can cut the attackers kill-chain before they're able to execute should be a critical part of defensive strategy for any protected asset, but especially in those that are part of the nation's critical infrastructure.

Conclusions

For critical systems that can be fully or partially isolated, testing the isolation should be a de-facto protection strategy. As with any defensive action, its correctness needs to be continuously monitored to avoid lulling into a false sense of security. In this case, a simple configuration mistake at firewall rules opened a network path to and from part of network thought to be isolated. Active network leak detection solution, in form of SensorFu Beacon, demonstrated capability to detect network misconfiguration, and alert appropriate stakeholders, be it IT staff, network administrators, security or network operations center (SOCs, NOCs), of the misconfiguration. This leads to a timely remediation of the problem. All Of This Has Happened Before And Will Happen Again.

If critical infrastructure protection is your responsibility, please contact us at contact@sensorfu.com for product information and to hear more about our experiences in protecting critical infrastructure and ensuring network isolation. More information about SensorFu Beacon is available at https://www.sensorfu.com/ .

[1] https://ccdcoe.org/exercises/locked-shields/
[2] https://ics-cert.us-cert.gov/Recommended-Practices
[3] Analysis of the Cyber Attack on the Ukrainian Power Grid - Defense use case
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
[4] Verizon data breach investigation report 2019 -
https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf