# Cybersecurity Tabletop Exercise

Goitom Weldehawaryat

# Outline

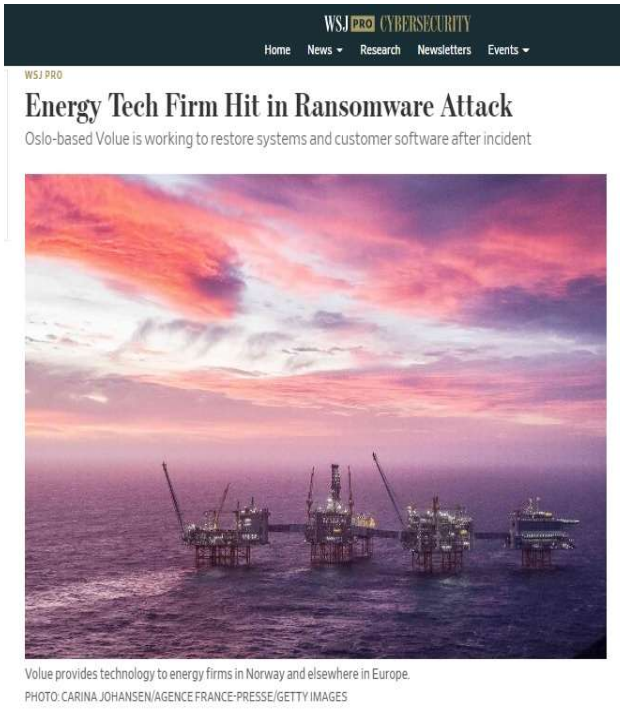
- Introduction
- Exercise objectives and guidelines
- Cybersecurity incident scenario(s)
- Start the exercise
- Feedback and closing comments

# Introduction

- The *water sector* consists of various utilities: water treatment, distribution and management.
- Like other critical infrastructures (e.g., smart grid), the water sector is increasingly *digitalised*, *networked* and *remotely managed* for automation, efficiency and functionality
- However, it results in increased *attack surface* and *risks* posed by cyber threat actors

# Cyber Incidents

- In May 2021, Volue was subject to a *cyber attack* that impacted its applications
- ***Ryuk Ransomware*** attack shut down applications providing infrastructure to *water and wastewater facilities* in 200 Norwegian municipalities, covering around 85 percent of the country's population
- The company shut down all other applications that it hosts and quarantined *around 200 employee devices* to prevent the *ransomware* from spreading to other computer systems



WSJ PRO

Energy Tech Firm Hit in Ransomware Attack

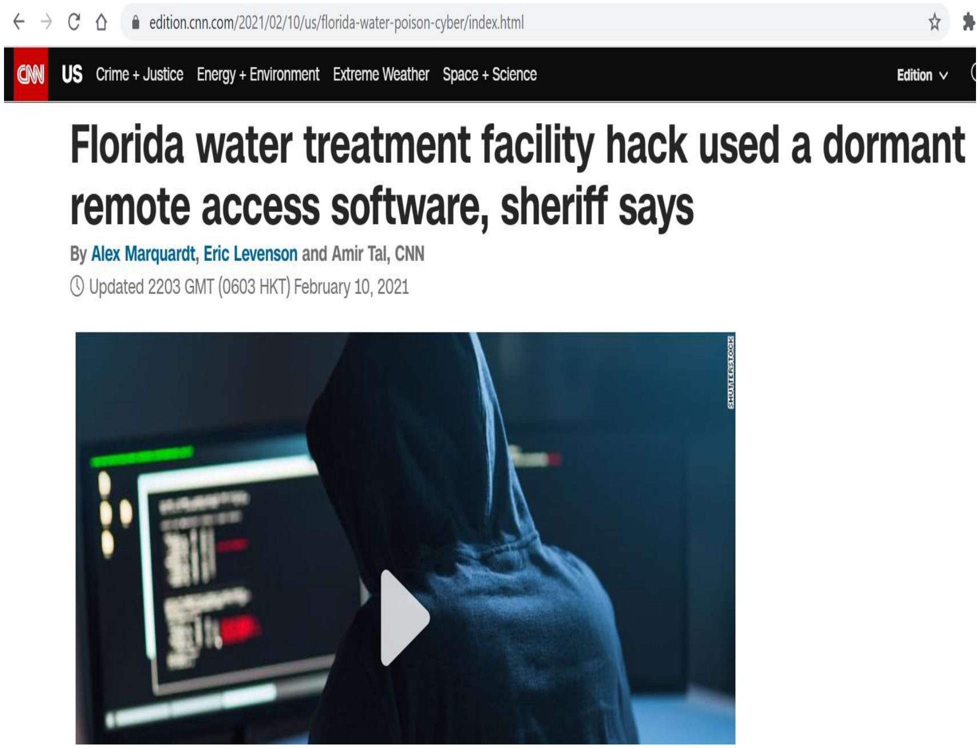
Oslo-based Volue is working to restore systems and customer software after incident

Volue provides technology to energy firms in Norway and elsewhere in Europe.

PHOTO: CARINA JOHANSEN/AGENCE FRANCE-PRESSE/GETTY IMAGES

# Cyber Incidents

- In February 2021, attackers accessed the control system's software at the **Oldsmar water-treatment** facility in Florida, and attempted to increase the levels of **sodium hydroxide (lye)** to more than 100 times its normal levels (100ppm to 11,100ppm )
- The attack used **stolen credentials** that were shared between multiple users and devices to remotely login to the *HMI* station controlling the water systems
- The change was immediately detected by a plant operator

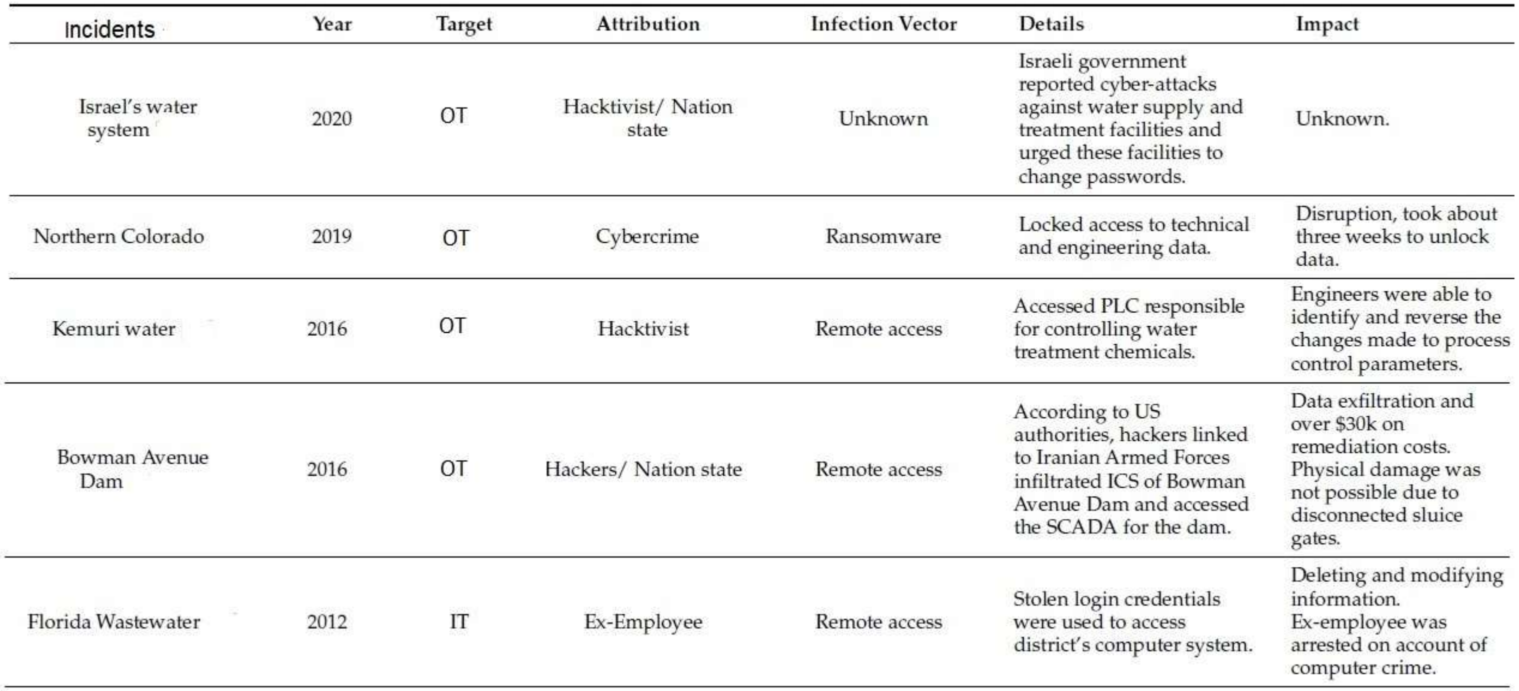


Florida water treatment facility hack used a dormant remote access software, sheriff says

By Alex Marquardt, Eric Levenson and Amir Tal, CNN

Updated 2203 GMT (0603 HKT) February 10, 2021

# Cyber Incidents



| Incidents | Year | Target | Attribution | Infection Vector | Details | Impact |
|---|---|---|---|---|---|---|
| Israel's water system | 2020 | OT | Hacktivist/ Nation state | Unknown | Israeli government reported cyber-attacks against water supply and treatment facilities and urged these facilities to change passwords. | Unknown. |
| Northern Colorado | 2019 | OT | Cybercrime | Ransomware | Locked access to technical and engineering data. | Disruption, took about three weeks to unlock data. |
| Kemuri water | 2016 | OT | Hacktivist | Remote access | Accessed PLC responsible for controlling water treatment chemicals. | Engineers were able to identify and reverse the changes made to process control parameters. |
| Bowman Avenue Dam | 2016 | OT | Hackers/ Nation state | Remote access | According to US authorities, hackers linked to Iranian Armed Forces infiltrated ICS of Bowman Avenue Dam and accessed the SCADA for the dam. | Data exfiltration and over $30k on remediation costs. Physical damage was not possible due to disconnected sluice gates. |
| Florida Wastewater | 2012 | IT | Ex-Employee | Remote access | Stolen login credentials were used to access district's computer system. | Deleting and modifying information. Ex-employee was arrested on account of computer crime. |

# Exercise Objectives

The cybersecurity exercise objectives include to:

- Explore *cybersecurity challenges* and suggest possible solutions
- Improve participants' roles and responsibilities for *managing the consequences of a cybersecurity incident*, which should be reflected in their plans, procedures, and other preparedness
- Increase *awareness* of the damage that can be caused by a cybersecurity incident on a business or control system
- Identify *enhancements* needed to the cybersecurity incident tabletop exercise and other *preparedness* elements currently in place

# Exercise Guidelines

- This exercise will be held in an open, no-fault environment – varying viewpoints are expected
- The basis for discussion consists of the *scenario description* and *modules*, your experience, your understanding of cyber incident, and other resources
- Suggestions and recommended actions that could improve *prevention, protection/detection, mitigation, response* or recovery efforts should be the focus
- This exercise is an opportunity to discuss and present multiple options and possible solutions

# Cybersecurity Incident  Scenario

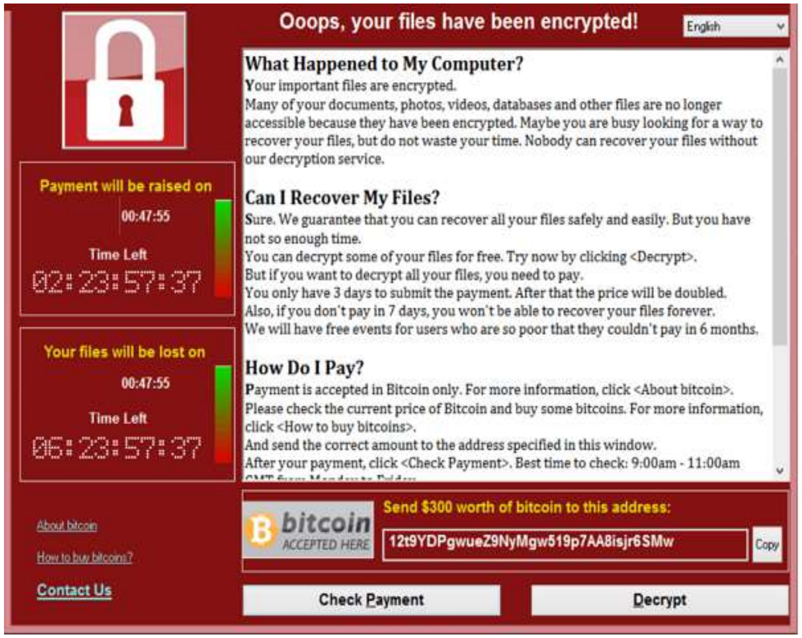
# Module 1 – a suspicious email

- [May 20, 2022:0800 hrs] *Jack* is an employee for a small water utility company in a small town. He receives an email with the subject title “Failed Package Delivery Notice” . *Jack* opens the email
- When *Jack* opened the email, he noticed that the recipient's name and address were not his, so he clicked the included link to find out more information
- The link took him to what appeared to be a blank webpage, but after a few seconds, it redirected him to *dhl.com*
- Lacking any more information on the package, he closed the email and continued to go about his business

# Module 1 – Key Issues

- *Jack* receives a suspicious email and clicks on the link

# Module 2 – a ransom message appears



**What Happened to My Computer?**

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

**Can I Recover My Files?**

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

**How Do I Pay?**

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

- [May 20, 2022:1100hrs] A few hours later, a message appears on *Jack*'s computer screen that reads “Your important files are encrypted”
- Files can be decrypted if a ransom for $300 is paid to receive a decryption key
- There is limited time to pay the ransom and get the key
- *Jack* sees all his files, but an error message appears when he tries to open them
- Afraid of disciplinary action, Jack decides to pay the ransom himself

# Module 2 – Key Issues

- The files on *Jack*'s computer are encrypted
- *Jack* does not notify anyone or seek advice before paying the ransom
- *Jack* did not check the files on the town's server, which he can access from his computer

# Module 3 – the malware spreads

- [May 20, 2022:1200hrs] *Jack* is panicked because he has not received the decryption key
- *Monica* asks *Jack* if he is having trouble accessing server files, as she is
- *Monica* is worried because the town's server holds six years of critical files and customer billing information needed for daily operations
- *Jack* breaks down and tells *Monica* about the ransom and that he still doesn't have the key

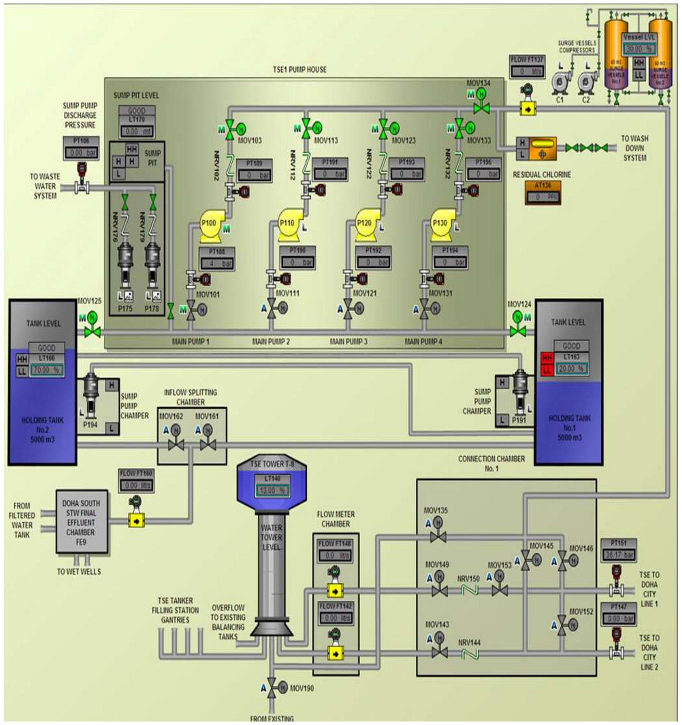
# Module 3 – the malware spreads (cont.)

- *Monica* responds to *Jack* that they must report the incident to their supervisor immediately
- They then call their IT vendor representative, *Martin* – he tells them to disconnect both Jack's computer and the infected server from the network
- *Martin* goes to *Jack*'s office and confirms that the files on both his computer and the town's server have been encrypted

# Module 3– Key Issues

- The malware has spread to the town server and all the files are encrypted
- Business operations are frozen until the files can be accessed
- *Jack* has not received the decryption key

# Module 4 – SCADA locked



- [May 20, 2022:1330hrs] *Martin* is working on *Jack*'s computer and the town's server when he receives an urgent call from the town's combined drinking water and wastewater treatment facility
- The operator  there has observed that the Supervisory Control and Data Acquisition (SCADA) control screens are not showing updated data
- Instead, the screens have frozen, and critical process information is not current

# Module 4 – SCADA locked (cont.)

- *Martin* believes that the utility's SCADA problems are due to the malware infection on *Jack*'s computer and the town's server
- *Martin* tells the operator that if possible, the drinking water and wastewater processes should be operated in a manual mode

# Module 4 – Key Issues

- The town server and the SCADA system for the drinking water and wastewater utility are connected through a flat network, which means there is no firewall regulating traffic between the server and the SCADA system
- The integrity of the SCADA system has been compromised by the malware infection – control screens are frozen, and utility process control system information is not being updated
- The utility must be operated in manual mode

# Module 5 – malware identified

- [May 20, 2022:1430hrs] After investigation, *Martin* confirms that the malware did spread across the flat network from the town server to the SCADA system
- The malware encrypted critical data and program files that the SCADA system needs

# Module 5 – Key Issues

- The malware encrypted critical data files that the SCADA system reads and uses for communications with operators and between processes
- *Martin* will need to investigate multiple components connected to the SCADA system to evaluate the extent of damage

# Module 6 – the system is restored

- [May 21, 2022:0730hrs] After confirming malware contamination, *Martin* backs up all the log files to keep a record of the incident
- He then wipes each infected computer and restores them with clean backups
- Next, *Martin* retrieves the last set of backups (one month old) for the town's server. he proceeds to restore the server from the backups
- Several errors are displayed.  *Martin* checks the backup drive, and realizes that some files are not readable

# Module 6 – the system is restored (Cont.)

- *Martin*, unable to proceed with a quick restoration, decides to do a full reinstallation and reconfiguration of the file server
- *Martin* works through the night to get the server back up and running
- *Martin* repeats these procedures at the utility, allowing the utility to switch back to automated operation

# Module 6 – Key Issues

- Backups were not routinely verified to ensure that they functioned as needed
- *Martin* conducts a full system restoration and wipes all workstations clean of the malware
- *Martin* reports the incident to ICS-CERT

Please start the exercise

# Feedback and closing comments

# References

- CISA. 2022. “CISA Tabletop Exercises Packages | CISA.” https://www.cisa.gov/cisa-tabletop-exercises-packages (May 27, 2022).

- Dean Parsons. 2021. “Top 5 ICS Incident Response Tabletops and How to Run Them | SANS Institute.” https://www.sans.org/blog/top-5-ics-incident-response-tabletops-and-how-to-run-them/ (May 25, 2022).

- EPA. 2022. “Cybersecurity Step 1 - Tabletop Exercise Tool for Drinking and Waste Water Utilities.” https://ttx.epa.gov/CyberSecurity1.html (May 25, 2022).

- Johnson, Leighton. 2020. “Security Component Fundamentals for Assessment.” *Security Controls Evaluation, Testing, and Assessment Handbook*: 471–536.

# Thank you for participating