WATER ISAC

Water Information Sharing and Analysis Center

WATER SECTOR CYBER RESILIENCE BRIEFING

January 24, 2024

Housekeeping

- This webinar is being recorded.

- The recording and slide deck **will be available** by tomorrow at waterisac.org/webcasts.

- There will be a Q&A session.

Request for Information

- *Do you have experience regarding **telecommunications infrastructure co-located with water infrastructure** and how you have granted access, but still protected your water supply?*
- *Have you had to balance pressure from councils or boards?*

Contact me directly walker@waterisac.org or other WaterISAC emails… info@waterisac.org or analyst@waterisac.org

CYBER RESILIENCE BRIEFING

WATER ISAC

Do You Struggle with OT/ICS Cybersecurity or Just Need a Sanity Check?

Wednesday, January 24 at 2 PM ET

SPEAKERS FROM DRAGOS

Dawn Cappelli, *Head of OT-CERT*

Gus Serino, *OT-CERT/I&C Secure*

DRAGOS

What’s Happenin’ in the WWS Sector?

- Unitronics PLC HMI defacements
- Ivanti Connect Secure VPN zero-day vulnerabilities
- Federal and Quasi-governmental Guidance &Initiatives
    - Federal Partners Release **Incident Response Guide for the Water and Wastewater Systems (WWS) Sector**
- Threat Activity
- WaterISAC's Quarterly Water Sector Incident Summary, July to September 2023

WWS Incidents

- Veolia North America *(hasn’t been posted to our portal yet)*
- UK Water Utility Acknowledges Threat Actor Claims of Stolen Data
- Daixin Team Ransomware Group Claims to Have Successfully Attacked Texas Water Utility
- Cyber Incident: Wastewater Agency in Paris, France Reports Attack
- Florida Water Agency Confirms Cyber Incident

CYBER RESILIENCE BRIEFING

WATER ISAC

Do You Struggle with OT/ICS Cybersecurity or Just Need a Sanity Check?

Wednesday, January 24 at 2 PM ET

SPEAKERS FROM DRAGOS

Dawn Cappelli, *Head of OT-CERT*

Gus Serino, *OT-CERT/I&C Secure*

DRAGOS

Cyber Updates

- Spotlight – *Andy Krapf, Loudoun Water, Virginia*
- **WWS Sector Activity**
  - Unitroincs
  - Ivanti Connect Secure VPN Vulnerabilities
  - Federal, etc. Guidance and Resources
  - WWS Incidents & Threats
- Active Threats & Vulnerabilities
- Government Reports & Resilience Resources
- General Cyber Resilience

WATER ISAC

Spotlight

- WaterISAC Recognizes Andrew Krapf as Splash Award Recipient (Read more)

WWS Sector Activity - Unitronics

- (TLP:CLEAR) Water Utility Control System Cyber Incident Advisory: ICS/SCADA Incident at Municipal Water Authority of Aliquippa (Updated November 30, 2023) (Read more)
- (TLP:CLEAR) CISA Releases Alert on Exploitation of Unitronics PLCs Used in Water and Wastewater Systems (Read more)
- WaterISAC Advisory: (TLP:CLEAR) CISA and Partners Confirm Additional Activity into Exploitation of Unitronics PLCs Across the U.S. Water and Wastewater Sector (Read more)
- ICS/OT Cybersecurity – Unitronics Issues Update to Recently Targeted PLCs (Read more)
- Continued Focus on Recent Cyber Incidents at “Small Town” Water Utilities (Read more)
- ICS/OT – (TLP:AMBER) Recent CyberAv3ngers Activity Hits Wastewater Treatment Control Screens at Transportation Entity (Read more)
- Irish Utility Experiences Water Disruption after Politically Motivated Threat Actor Compromises Israeli Pumping System (Read more)

WWS Sector Activity – Ivanti Connect Secure VPN Vulnerabilities

- WaterISAC Advisory: CISA Issues Emergency Directive on Ivanti Vulnerabilities (Read more)
- Vulnerability Notification – Active Zero-Day Exploitation of Ivanti Connect Secure and Policy Secure Gateways (Update: January 16, 2024) (Read more)

WWS Sector Activity – Federal and Quasi-governmental Guidance Resources and Initiatives

- Cyber Resilience: Federal Partners Release Incident Response Guide for the Water and Wastewater Systems (WWS) Sector (Read more)
- Microsoft and Cyberspace Solarium Commission Address Urgent Water Infrastructure Cybersecurity Threats with Multistakeholder Solutions (Read more)
- New CISA Infrastructure Resilience Planning Framework Case Studies Includes Water & Wastewater Use Case (Read more)
- Cyber Resilience: OIG Report on Improving Collaboration to Enhance Cyber Resiliency in the Water and Wastewater Sector (Read more)
- CISA Launches Targeted Pilot Program for Critical Infrastructure, including Water and Wastewater Sector (Read more)

WWS Incidents & Threats

- Veolia North America *(hasn't been posted to our portal yet)*
- Incident Awareness – UK Water Utility Acknowledges Threat Actor Claims of Stolen Data (Read more)
- Daixin Team Ransomware Group Claims to Have Successfully Attacked Texas Water Utility (Read more)
- Cyber Incident: Wastewater Agency in Paris, France Reports Attack (Read more)
- Florida Water Agency Confirms Cyber Incident (Read more)

Active Threats & Vulnerabilities

- Outlook Exploitation
  - Threat Awareness – Outlook Calendar Invite Vulnerability Can Steal Passwords with One Click (Read more)
  - Microsoft Outlook Zero-Click Security Flaws Triggered by Sound File (Read more)
  - Russian APT28 Exploits Outlook Bug to Access Exchange (Read more)
- Social Engineering
  - Cyber-Physical Security Awareness – Effective Social Engineering Tricks that Still Work (Read more)
  - Security Awareness – New Year, Old Themes (Read more)

Government Reports & Resilience Resources

- CISA Urges Manufacturers Eliminate Default Passwords to Thwart Cyber Threats (Read more)
- NSA Releases Recommendations to Mitigate Software Supply Chain Risks (Read more)
- Joint Cybersecurity Advisory – #StopRansomware: Play Ransomware (Read more)
- Joint Cybersecurity Advisory – #StopRansomware: ALPHV Blackcat (Read more)
- Joint Cybersecurity Advisory - Karakurt Data Extortion Group (Updated December 14, 2023) (Read more)
- (U//FOUO) Russia: Likely Capable of Disrupting US Critical Infrastructure by Compromising Satellite Communications (Read more)
- CISA and FBI Release Cybersecurity Guidance: Chinese-Manufactured UAS (Read more)
- CISA and FBI Release Known IOCs Associated with Androxgh0st Malware (Read more)

WATER ISAC

General Cyber Resilience

- It’s Data Privacy Week 2024 – Take Control of your Data (Read more)
- Ransomware Resilience – Don’t Wait ‘til it’s Too Late (Read more)
- Ransomware Resilience – You Can’t Handle Not Exercising (Ransomware Response) (Read more)

Upcoming WaterISAC Events

Water Sector Cyber Resilience Briefing

- Wednesday, February 28, 2024, 2:00 – 3:00 PM ET

Register for all events via WaterISAC's Events webpage:
https://www.waterisac.org/events

Incident Reporting

Please report incidents and suspicious activity to WaterISAC

- ❑ **1-866-H2O-ISAC**
- ❑ **https://www.waterisac.org/report-incident**
- ❑ **analyst@waterisac.org**

Thank you!

WaterISAC Contact Information:

1-866-H2O-ISAC

Tom Dobbins
Executive Director
dobbins@waterisac.org

Charles Egli
Preparedness and Response Director
egli@waterisac.org

Alec Davison
All-Hazards Risk Analyst
davison@waterisac.org

Kaitlyn Palatucci
Membership Engagement Director
palatucci@waterisac.org

Jennifer Lyn Walker
Infrastructure Cyber Defense Director
walker@waterisac.org

Andrew Hildick-Smith
OT Security Lead
hildick-smith@waterisac.org

April Zupan
All-Hazards Risk Analyst
zupan@waterisac.org

WWW.WATERISAC.ORG

WATER ISAC