OFFICE of INTELLIGENCE and ANALYSIS
INTELLIGENCE IN BRIEF
11 FEBRUARY 2022 DHS-IA-IB-2022-01142

CYBERSECURITY

(U//FOUO) California Water and Wastewater Sector Remains Attractive Target for Cyber Actors

(U//FOUO) ***Scope Note:*** *This* Intelligence in Brief *is intended for public and private sector partners in California to provide awareness of the cyber threat to California's water and wastewater sector. This assessment is tailored specifically for California partners and takes into consideration recent drought and wildfire conditions throughout the state as a possible motivation for malicious cyber actors. The DHS Office of Intelligence and Analysis, in partnership with the California Cybersecurity Integration Center, the California State Threat Assessment Center, and the Northern California Regional Intelligence Center, plans to conduct additional analysis on this topic, examining scenarios in which a malicious cyber actor could compromise a California water sector entity and disrupt water services.*

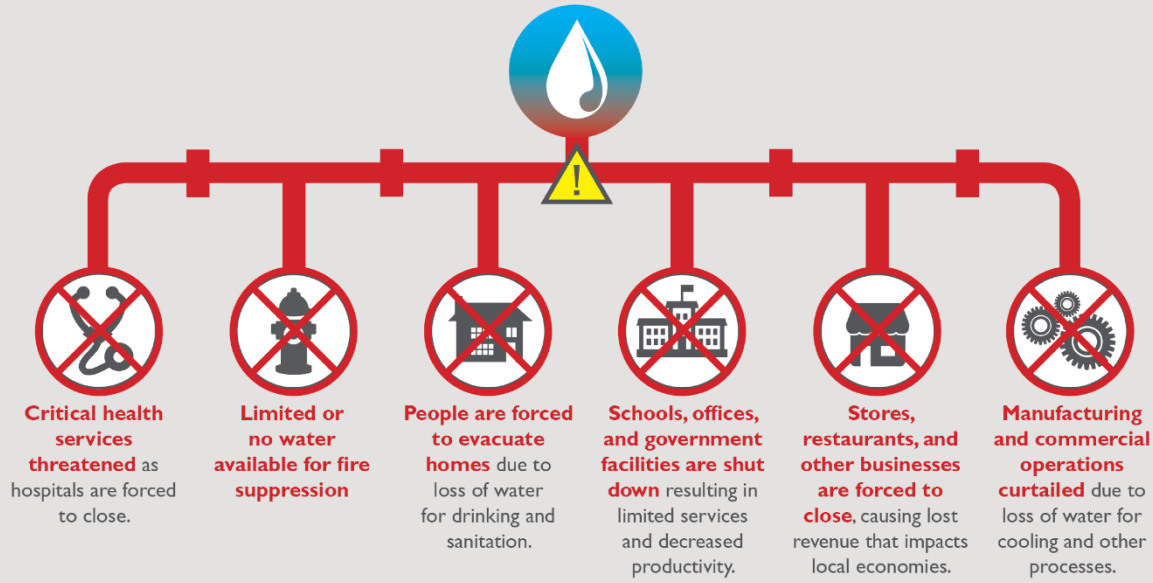
(U//FOUO) **We assess that the California water and wastewater sector likely will remain an attractive target for a range of cyber actors seeking to exploit enduring vulnerabilities to achieve their financial, geopolitical, or ideological objectives.** During 2021, unidentified cyber actors targeted multiple water sector entities in California using data deletion malware, ransomware, and other routine malicious cyber tactics. At least one of these compromises temporary disrupted automation of water control systems. This assessment assumes that some cyber actors are aware of California's distinctive water needs—particularly during extreme drought and prolonged wildfire seasons—and consider these conditions as favorable for exploitation.

- *(U//FOUO)* In August 2021, unidentified cyber actors compromised a California water sector entity's network, inhibiting automation of water control systems for an unspecified period of time, according to a US state cybersecurity analyst. The cyber actors exploited a vulnerability in the virtual private network and ran a malicious command to delete volume shadow copies on the network's primary domain controller (PDC) and supervisory control and data acquisition (SCADA) server. The malicious activity wasn't detected until a base64 encoded program was run from the PDC, which appeared to be executed from a commercially

(U) Prepared by the Field Operations Division – Central Pacific Region, the Cal-CSIC, NCRIC, and the STAC. Coordinated within the DHS Intelligence Enterprise (CISA and CYMC). For questions, contact DHS-SPS-RFI@hq.dhs.gov.

available command and control penetration testing tool. The execution of the malicious code coincided with another task that deployed a variant of Ghost ransomware and encrypted files on the SCADA servers and PDC.

- *(U//FOUO)* In June 2021, unidentified cyber actors used a compromised or spoofed e-mail address of a California-based water sector entity to phish a municipal government employee, according to a US local law enforcement analyst. The e-mail contained a link to preview a PDF that, if clicked, led to a webpage containing the Microsoft Office 365 and Adobe PDF logos alongside a "click here to view document" prompt. If the prompt were clicked, the user would be prompted to enter Office 365 credentials.
- *(U//FOUO)* In January 2021, unidentified cyber actors compromised a northern California-based water sector entity network and deployed ransomware that encrypted data on servers, several workstations, and the first and second layers of backup systems, according to a US local law enforcement analyst. In a separate incident in January, unidentified cyber actors used a former employee's login credentials to remotely access a northern California-based water treatment facility network and deleted software that monitored and managed various components and processes used to provide clean water, according to the same US local law enforcement analyst.



(U) When water and wastewater services are lost, even for short periods, the consequences can be widespread and significantly degrade the functionality of multiple interdependent sectors, according to a National Infrastructure Advisory Council (NIAC) water sector resilience report. The effects of extended service disruptions can be catastrophic. Significant points of interdependencies include: chemical, energy, communications, information technology, and transportation sectors.[a]

[a] *(U)* For recommended mitigation, please see Joint Cybersecurity Advisory, "Ongoing Cyber Threats to U.S. Water and Wastewater Systems (AA21-287A)" dated 14 October 2021.

Source, Reference, and Dissemination Information	
Source Summary Statement	*(U//FOUO)* We assess that the California water and wastewater sector likely will remain an attractive target for a range of cyber actors seeking to exploit enduring vulnerabilities to achieve their financial, geopolitical, or ideological objectives. We have **low confidence** in this assessment. Our confidence is derived from a body of DHS reports; a NIAC water sector resilience report; and an article from a US-based, non-profit news media agency. We consider the DHS reports credible and important to our analysis as they provided incident insights that are not publicly available and are helping us evaluate the developing threat landscape of malicious cyber activity targeting California water entities. The NIAC report offered critical, in-depth analysis and sector-specific, expert insights into the consequences of water service disruptions. Moreover, understanding the impact of water service disruptions was important as we examined plausible motivations and was key when considering the assumption that cyber actors are aware of California's distinctive water needs. Conclusive attributions, and in some cases, end objectives, of the malicious cyber activity targeting California's water sector in 2021 remain an intelligence gap. Conclusive attribution would help us better evaluate the actors' intent and capabilities and contribute to stronger confidence in this assessment.
Reporting Suspicious Activity	*(U)* To report incidents of concern to the Intelligence Community, please contact your DHS I&A Field Operations officer at your state or major urban area fusion center, or e-mail DHS.INTEL.FOD.HQ@hq.dhs.gov. DHS I&A Field Operations officers are forward deployed to every US state and territory and support state, local, tribal, territorial, and private sector partners in their intelligence needs; they ensure any threats, incidents, or suspicious activity is reported to the Intelligence Community for operational awareness and analytic consumption.
Dissemination	*(U)* Federal, state, local, tribal, territorial authorities and private sector partners.
Warning Notices & Handling Caveats	*(U)* **Warning**: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials **may share** this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS. *(U)* All US person information has been minimized. Should you require US person information on weekends or after normal weekday hours during exigent and time sensitive circumstances, contact the Current and Emerging Threat Watch Office at 202-447-3688, CETC.OSCO@HQ.DHS.GOV. For all other inquiries, please contact the Homeland Security Single Point of Service, Request for Information Office at DHS-SPS-RFI@hq.dhs.gov, DHS-SPS-RFI@dhs.sgov.gov, DHS-SPS-RFI@dhs.ic.gov.

Homeland Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title: (U//FOUO) California Water and Wastewater Sector Remains Attractive Target for Cyber Actors

All survey responses are completely anonymous. No personally identifiable information is captured unless you voluntarily offer personal or contact information in any of the comment fields. Additionally, your responses are combined with those of many others and summarized in a report to further protect your anonymity.

1. Please select partner type: Select One **and function:** Select One

2. What is the highest level of intelligence information that you receive? Select One

3. Please complete the following sentence: "I focus most of my time on:" Select One

4. Please rate your satisfaction with each of the following:

	Very Satisfied	Somewhat Satisfied	Neither Satisfied nor Dissatisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Product's overall usefulness	○	○	○	○	○	○
Product's relevance to your mission	○	○	○	○	○	○
Product's timeliness	○	○	○	○	○	○
Product's responsiveness to your intelligence needs	○	○	○	○	○	○

5. How do you plan to use this product in support of your mission? ***(Check all that apply.)***

- ☐ Drive planning and preparedness efforts, training, and/or emergency response operations
- ☐ Observe, identify, and/or disrupt threats
- ☐ Share with partners
- ☐ Allocate resources (e.g. equipment and personnel)
- ☐ Reprioritize organizational focus
- ☐ Author or adjust policies and guidelines
- ☐ Initiate a law enforcement investigation
- ☐ Intiate your own regional-specific analysis
- ☐ Intiate your own topic-specific analysis
- ☐ Develop long-term homeland security strategies
- ☐ Do not plan to use
- ☐ Other:

6. To further understand your response to question #5, please provide specific details about situations in which you might use this product.

7. What did this product *not* address that you anticipated it would?

8. To what extent do you agree with the following two statements?

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree	N/A
This product will enable me to make better decisions regarding this topic.	○	○	○	○	○	○
This product provided me with intelligence information I did not find elsewhere.	○	○	○	○	○	○

9. How did you obtain this product? Select One

10. Would you be willing to participate in a follow-up conversation about your feedback? Yes

To help us understand more about your organization so we can better tailor future products, please provide:

Name: *Position:*
Organization: *State:*
Contact Number: *Email:*

Submit Feedback

Privacy Act Statement

Product Serial Number: DHS-IA-IB-2022-01142 REV: 10 November 2016