Homeland Security
OFFICE of INTELLIGENCE and ANALYSIS
NETWORK DEFENDER BULLETIN

11 AUGUST 2022 DHS-IA-NDB-2022-16474

CYBERSECURITY

(U//FOUO) Northeast Wastewater Facility Targeted With Ransomware

(U//FOUO) ***Scope Note:*** *This* Network Defender Bulletin *provides federal, state, local, and private sector network defenders information to help detect and mitigate malicious cyber activity. While I&A considers this network defense information to be credible and actionable, this* Bulletin *is not considered finished intelligence and is being shared for the purpose of informing cybersecurity protection activities.*

(U//FOUO) In July 2022, the ransomware group Monti targeted a northeast wastewater facility's business networks with a possible new ransomware variant that impacted 9 physical servers and 100 virtual servers, preventing employees from accessing them, according to a government report. The group accessed the facility's networks through VMware Horizon servers vulnerable to the Log4j vulnerability and changed VMware host passwords, rendering the facility's main backup and secondary backup servers inaccessible, according to the same report. The group deleted a year of backup data, but no operational technology was affected. The group also claimed to have exfiltrated data from the facility, but, as of the time of reporting, this had not been confirmed; as of 20 July 2022, the facility was largely operational, according to the same report.

(U) Support to Computer Network Defense

This table is UNCLASSIFIED//FOR OFFICIAL USE ONLY

Indicator of Compromise	Value
Locker.exe	b88b5e16c412251d79ad13c8fa94daa735fbaa2c
AnyDesk	9779751121508f17cbd831e9c2780b4cf0e1b96c
Secretsdump.exe	af7c73c47c62d70c546b62c8e1cc707841ec10e3
WinSCP.exe	6a595fe76467cd5f67c2f9960a8b8af0ec186a5b
netscan64.exe	N/A
mimikatz.exe	N/A
putty.exe	N/A
action1_agent.exe	f2be59a51ed98560c497cbeb6d3a6a18a41c5f60
action1_remote.exe	cabef042e4f6eabc32aea0025e61f51defba28c3
meshagent.exe	4bdada55a9d2bc5914eceacdab01e467be1f998d
winagent-v2.0.4.exe	602befd718736d2b02f2e3654d6ce297dd9814a5
p.exe	b97761358338e640a31eef5e5c5773b633890914
hplick.exe	2303677459f7e5010e495e2ac87f6e66b1b54cd2
7za.exe	bbe24cbae89166de829a7cf91eebfb518d8f45be
Log4j	CVE-2021-44228
.puuuk	Malicious file extension

(U) Prepared by the Cyber Mission Center. For questions, contact DHS-SPS-RFI@hq.dhs.gov

Source, Reference, and Dissemination Information	
Reporting Suspicious Activity	*(U)* To report this incident to the Intelligence Community, please contact your DHS I&A Regional Intelligence officer at your state or major urban area fusion center, or e-mail DHS.INTEL.ORI.HQ@hq.dhs.gov. DHS I&A Regional Intelligence 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. *(U)* To report a computer security incident, please contact CISA at 888-282-0870; or go to https://forms.us-cert.gov/report. The CISA Incident Reporting System provides a secure web-enabled means to report computer security incidents to CISA. This system assists analysts in providing timely handling of your security incidents, as well as the ability to conduct improved analysis. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.
Dissemination	*(U)* Federal, state, local, and private sector network defenders.
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)* US person information has been minimized. 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. *(U//FOUO)* This report includes sensitive technical information related to computer network operations that could be used against US Government information systems. Any scanning, probing, or electronic surveying of IP addresses, domains, e-mail addresses, or user names identified in this document is strictly prohibited.

CLASSIFICATION: **UNCLASSIFIED//FOR OFFICIAL USE ONLY**

Homeland Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title: (U//FOUO) Northeast Wastewater Facility Targeted With Ransomware

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

CLASSIFICATION: **UNCLASSIFIED//FOR OFFICIAL USE ONLY**