STATE OF CONNECTICUT
DEPARTMENT OF PUBLIC HEALTH

Manisha Juthani, MD
Commissioner

Ned Lamont
Governor
Susan Bysiewicz
Lt. Governor

Environmental Health and Drinking Water Branch

EHDW Circular Letter #2022-59

TO: Community Public Water Systems

FROM: Lori Mathieu, Public Health Branch Chief, EHDW Lori J. Mathieu '22

DATE: September 28, 2022

SUBJECT: **CISA and FBI Advisory on Iranian State Actors Conduct Cyber Operations Against the Government of Albania**

The Department of Public Health (DPH) Drinking Water Section (DWS) wants to inform that the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) released a joint Cybersecurity Advisory (CSA) with technical details on cyber activity by Iranian state actors that launched a destructive cyberattack against the government of Albania. The cyberattack included ransomware and disk wiper, rendering websites and services unavailable in July 2022. The advisory provides details on the attribution, timeline of activity observed (approximately 14 months), from initial access to execution of the encryption and wiper attacks, and technical details on the ransomware cryptor, disk wiper, and additional files related to this activity.

Between May and June 2022, Iranian state cyber actors conducted lateral movements, network reconnaissance, and credentials harvesting from Albanian government networks. In July 2022, the actors, claiming to be a group named HomeLand Justice, launched ransomware on the networks, leaving an anti Mujahideen E-Khalq (MEK) message on the desktop. When network defenders identified and began to respond to the ransomware activity, the cyber actors deployed a version of ZeroCleare destructive malware.

In the CSA, CISA and FBI are providing host-based and network-based indicators of compromise (IOCs) that can be used by organizations / Public Water Systems (PWSs) to detect if this malicious activity is on their networks. The recommended mitigations include:

- Ensure anti-virus and anti-malware software is enabled and signature definitions are updated regularly and in a timely manner. Well-maintained anti-virus software may prevent use of commonly deployed attacker tools that are delivered via spear-phishing.
- Adopt threat reputation services at the network device, operating system, application, and email service levels. Reputation services can be used to detect or prevent low-reputation email addresses, files, URLs, and IP addresses used in spear-phishing attacks.
- If your organization is employing certain types of software and appliances vulnerable to known Common Vulnerabilities and Exposures (CVEs), ensure those vulnerabilities are patched.
- Monitor for unusually large amounts of data (i.e., several GB) being transferred from a Microsoft Exchange server.
- Check the host-based indications, including webshells, for positive hits within your environment. The advisory provides details on the attribution

All organizations / PWSs are encouraged to review the CSA for complete details on this ongoing threat and recommended mitigations. For more information on state Iranian malicious cyber activity, see CISA's Iran Cyber Threat Overview and Advisories webpage.
This advisory is available on stopransomware.gov, a one-stop hub with other advisories on ransomware threat and no-cost resources for individuals, businesses, and other organizations.
The StopRansomware.gov is a collaborative effort across the federal government to help private and public organizations mitigate their ransomware risk.

All organizations / PWS should share information on incidents and anomalous activity to CISA 24/7 Operations Center at report@cisa.gov or Report | CISA and/or to the FBI via your local FBI field office or the FBI's 24/7 CyWatch at (855) 292-3937 or CyWatch@fbi.gov. State, local, tribal, and territorial (SLTT) organizations should report incidents to MS-ISAC (866-787-4722 or SOC@cisecurity.org).

c: Heather Aaron, Deputy Commissioner, DPH