Hive Pro®

Threat Level

Red

CISA: AA23-335A

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

Iranian APT Group 'CyberAv3ngers' Target U.S. Critical Infrastructure

Date of Publication	Admiralty code	TA Number
December 5, 2023	A1	TA2023486

Summary

First Appearance: 2020
Actor Name: CyberAv3ngers (also known as CyberAveng3rs, Cyber Avengers)
Target Industries: Critical Infrastructure (specifically Water and Wastewater Systems), Energy, Food and Beverage, Manufacturing, Healthcare, and Shipping
Target Region: United States of America and Israel
Malware: Crucio Ransomware

Actor Map

Actor Details

#1

CyberAv3ngers, also known as CyberAveng3rs or Cyber Avengers, is an Iranian Advanced Persistent Threat (APT) group affiliated with the Islamic Revolutionary Guard Corps (IRGC). This cyber persona has gained notoriety for its involvement in numerous cyberattacks, particularly targeting critical infrastructure organizations. The group has been active since at least 2020 and has claimed responsibility for various cyber incidents, especially against organizations in Israel.

#2

Notably, CyberAv3ngers is associated with the IRGC, an Iranian military organization that the United States designated as a foreign terrorist organization in 2019. The group uses tactics, techniques, and procedures (TTPs) aligned with state-sponsored cyber espionage, and its activities are often linked to geopolitical motivations, expressing opposition to Israel.

#3

The CyberAv3ngers group has a history of making false claims about compromising critical infrastructure organizations in Israel. Their operations have involved defacement messages and the use of ransomware, such as the "Crucio" ransomware, to disrupt systems and networks. The group is also reported to have connections with another IRGC-linked group called Soldiers of Solomon.

#4

In recent months, the CyberAv3ngers have expanded their target range to include the United States. In November 2023, they began targeting U.S.-based water and wastewater facilities that use Unitronics PLCs. The group has compromised these PLCs by exploiting default passwords and exposing them to the internet. Once they have gained access to a PLC, the CyberAv3ngers will often deface the HMI with messages like "You have been hacked, down with Israel."

#5

The CyberAv3ngers are a skilled and determined group of hackers. They are able to gain access to well-defended systems and cause significant disruption. It is important to be aware of the threat they pose and to take steps to protect your organization from their attacks.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
CyberAv3ngers (also known as CyberAveng3rs, Cyber Avengers)	Iran **MOTIVE** Information theft and espionage	United States of America and Israel	Critical Infrastructure (specifically Water and Wastewater Systems), Energy, Food, Beverage, Manufacturing, Healthcare, and Shipping

Recommendations

Change Default Passwords: Immediately change all default passwords on programmable logic controllers (PLCs) and human-machine interfaces (HMIs) to strong, unique passwords. Ensure that default passwords, especially those associated with Unitronics PLCs, are not in use.

Disconnect PLCs from Public-Facing Internet: Minimize exposure by disconnecting PLCs, especially those with internet-facing configurations, from public-facing internet access. Consider implementing network segmentation to isolate critical infrastructure devices from external networks.

Implement Multifactor Authentication (MFA): Introduce multifactor authentication for access to operational technology (OT) networks, especially for remote access. If remote access is necessary, employ a firewall and/or virtual private network (VPN) to control network access, and ensure the use of MFA.

Maintain Updated Software: Regularly update and patch PLCs, HMIs, and related controllers with the latest versions provided by the manufacturer.
Ensure that all devices in the operational technology environment are running the most current and secure software versions.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0006 Credential Access	TA0007 Discovery	TA0001 Initial Access
TA0040 Impact	T1110 Brute Force	T1584 Compromise Infrastructure	T1552 Unsecured Credentials
T1190 Exploit Public-Facing Application	T1057 Process Discovery	T1486 Data Encrypted for Impact	

Indicator of Compromise (IOCs)

TYPE	VALUE
SHA256	440b5385d3838e3f6bc21220caa83b65cd5f3618daea676f271c3671650ce9a3
SHA1	66AE21571FAEE1E258549078144325DC9DD60303
MD5	BA284A4B508A7ABD8070A427386E93E0
IPv4	178.162.227[.]180 185.162.235[.]206

References

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a

https://www.cisa.gov/news-events/alerts/2023/11/28/exploitation-unitronics-plcs-used-water-and-wastewater-systems

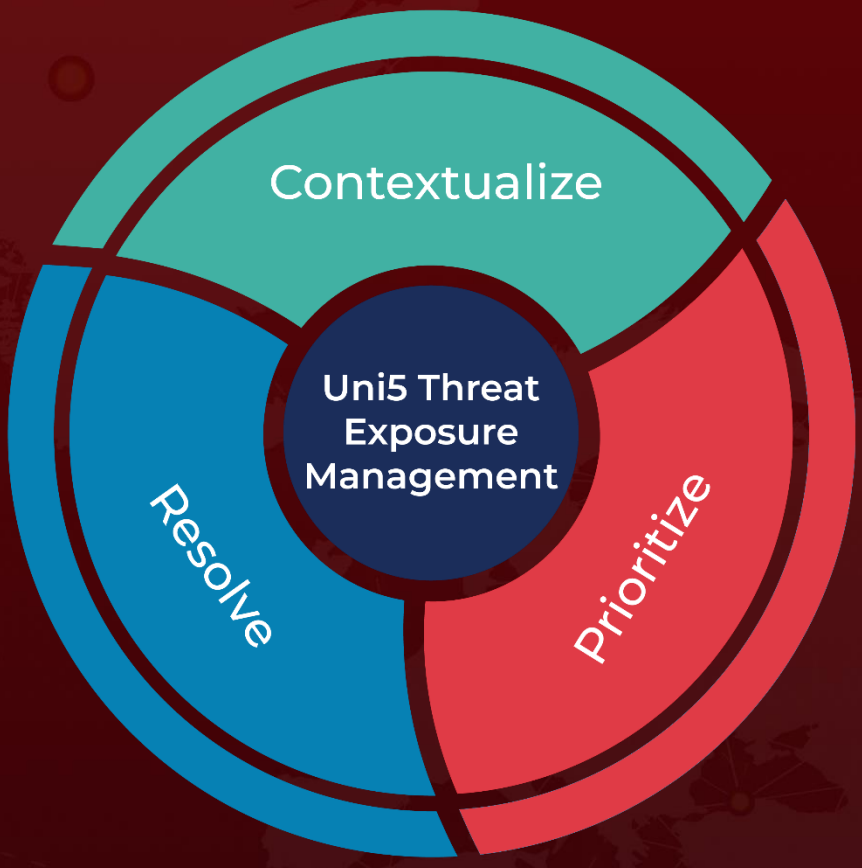
https://industrialcyber.co/industrial-cyber-attacks/iranian-hacker-group-cyberav3ngers-allegedly-breach-municipal-water-authority-of-aliquippa/

https://twitter.com/FalconFeedsio/status/1713467552771321981

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

December 5, 2023 . 4:30 AM

© 2023 All Rights are Reserved by Hive Pro ®

More at www.hivepro.com