American Hospital Association™
Advancing Health in America

Cybersecurity Advisory

August 29, 2024

Iran-based Cyber Actors Enabling Ransomware Attacks on U.S. Organizations

The FBI, Cybersecurity and Infrastructure Agency and the Department of Defense Cyber Crime Center today issued a joint advisory to warn of Iranian-based cyber actors leveraging unauthorized network access to U.S. organizations, including health care organizations, to facilitate, execute and profit from future ransomware attacks by apparently Russian-affiliated ransomware gangs. The Iranian group, which is associated with the Government of Iran, has conducted a high volume of cyberattack attempts on U.S. organizations since 2017 and as recently as August 2024. Based on an FBI assessment, the cyber actors obtain network access for espionage reasons then collaborate with ransomware groups, including the notorious Russian-linked ransomware groups RansomHub and APLHV aka BlackCat, to execute ransomware attacks against the espionage target. BlackCat was responsible for the 2024 Change Healthcare ransomware attack, the largest and most consequential cyberattack in U.S. history. The advisory does not indicate if the Iranian actors had any role in the Change Healthcare attack but does state that the Iranian group's ransomware activities are not likely sanctioned by the Government of Iran.

The joint advisory provides tactics, techniques, procedures, and indicators of compromise obtained from FBI investigations and third-party reporting. The federal agencies urge organizations to apply the recommendations in the mitigations section of the advisory to reduce the likelihood of compromise from these Iranian-based cyber actors and other ransomware attacks.

"This alert demonstrates the close 'international cooperation' between hackers to exploit cyber espionage campaigns for criminal profit," said John Riggi, AHA national advisor for cybersecurity and risk. "This alert also demonstrates the nation-state level sophistication and expertise of the ransomware groups that target U.S. health care. No health care organization, regardless of their cybersecurity preparedness, can be expected to fully defend against a group of nation-state-trained hackers collaborating with sophisticated ransomware gangs. Clearly, the initial access leading to a subsequent ransomware attack, sanctioned or not, is state-sponsored. We strongly encourage the U.S. government to treat these attacks as national security threats, by policy and action, and impose significant risk and consequences on our cyber adversaries. Offense is the best defense."

Although there is no specific threat information at this time, the field is reminded to remain especially vigilant over the holiday weekend, as we have historically seen increased targeting of health care around the holidays.

Please share this information with your IT and cyber infrastructure teams.

WHAT YOU CAN DO

- **Share** this advisory with your IT and cyber infrastructure teams.
- **Implement** the voluntary consensus-based health care sector cybersecurity performance goals.
- **Review** the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients resources.
- **Update** software and operating systems regularly to patch vulnerabilities.
- **Implement** strong email security measures to prevent phishing attacks.
- **Limit** account access privileges across organizations.
- **Protect** against threats using a combination of antivirus, anti-malware and firewall solutions.
- **Back up** data frequently and ensure backups are isolated and immutable.
- **Conduct** cybersecurity awareness training for employees to recognize and report suspicious activities such as phishing attempts.
- **Monitor** networks for suspicious activity and have an incident response plan in place.
- **Establish and implement** a business continuity plan to ensure minimal operational disruptions in case of a ransomware incident.

Additional details on mitigation strategy can be found on the Cybersecurity and Infrastructure Security Agency's #StopRansomware page.

FURTHER QUESTIONS

If you have further questions, please contact John Riggi, AHA's national advisor for cybersecurity and risk, at jriggi@aha.org. For the latest cyber threat intelligence and resources, visit www.aha.org/cybersecurity.