American Hospital Association™
Advancing Health in America

Cybersecurity Advisory

January 26, 2023

FBI Disrupts 'Hive' Ransomware Gang that Targeted Hospitals, Other Critical Infrastructure

The Department of Justice today announced major law enforcement action to disrupt the Hive ransomware gang that has targeted hospitals and other critical infrastructure.

The Hive gang used a ransomware-as-a-service (RaaS) model to attack organizations, with administrators developing ransomware strains and easy-to-use interfaces before recruiting affiliates who then access and encrypt victims' networks after exfiltrating sensitive data. Hive's developers and affiliates employed a double-extortion model of attack, wherein sensitive data from victims' systems was exfiltrated before encryption. The affiliate then sought a ransom for both the decryption key necessary to decrypt the victim's system and a promise to not publish the stolen data. Victims' most sensitive data was typically targeted to increase the pressure to pay.

In his media briefing, Attorney General Merrick B. Garland cited the case of a hospital located in the Midwest U.S. who, following a Hive attack, resorted to analog methods to treat existing patients and was unable to accept new patients for a period of time.

"The disruption and dismantlement of the notorious Hive ransomware operation by the FBI, the Department of Justice and international partners is welcome news and will no doubt help make hospitals safer against high-impact ransomware attacks that have disrupted health care's delivery and risked patient safety," said John Riggi, AHA's national advisor for cybersecurity and risk. "As Attorney General Garland stated, this coordinated international law enforcement action was assisted with victim cooperation, including hospitals, and through the robust exchange of cyber threat information exchange with the private sector.

"The AHA is proud to partner with all federal law enforcement, health care and national security agencies to facilitate and amplify the rapid and effective exchange of cyber threat information with the field — to help defend health care and the nation against these sinister cyber threats. We are also pleased to see the federal government prioritize ransomware attacks against hospitals as threat-to-life crimes and, and just as we did in the war on terrorism utilize a combination of law enforcement and intelligence authorities and capabilities to take down the bad guys. For the past several years we have publicly and privately advocated for implementation of this strategy to help hospitals defend against these threats and send a message to the bad guys: you can't conduct attacks which threaten public health and safety without drawing the full attention of the U.S. government and our allies, who will seek you out and impose consequences."

FURTHER QUESTIONS

If you have further questions, please contact John Riggi, AHA's national advisor for cybersecurity and risk, at jriggi@aha.org.