Joint CISA/NSA/FBI BlackMatter Ransomware Amplify Alert

Executive Summary
The Cybersecurity & Infrastructure Security Agency (part of the Department of Homeland Security) along with the National Security Agency and Federal Bureau of Investigation released a joint alert on BlackMatter ransomware. The alert acknowledged the BlackMatter group is likely a rebranding of the DarkSide group which, among other targets, is known for launching a ransomware attack which temporarily shut down the Colonial Pipeline in May of 2021. The alert provides technical details including indicators of compromise as well as mitigation and defensive recommendations.

Report
Alert (AA21-291A) BlackMatter Ransomware
https://us-cert.cisa.gov/ncas/alerts/aa21-291a

Impact to HPH Sector
BlackMatter, as all ransomware operators, poses a significant threat to the healthcare and public health (HPH) sectors. Healthcare provides an enticing target for both extorting ransom demands as well as stealing and selling protected health information (PHI) on the dark web. HC3 recommends health sector organizations take into consideration BlackMatter, as well as other ransomware threats, as they implement and maintain their risk management plans.

References
FBI, CISA, NSA shares defense tips for BlackMatter ransomware attacks

CISA, FBI, and NSA warn of BlackMatter attacks on agriculture and other critical infrastructure

NSA, FBI, CISA Issue Advisory on ‘BlackMatter’ Ransomware

A joint advisory officially associates the notorious ransomware-as-a-service group with the Colonial Pipeline attack.

Contact Information
If you have any additional questions, please contact us at HC3@hhs.gov.