USDOJ Dismantles International Ransomware Network

2/28/2023

The U.S. Department of Justice (DOJ) announced its "months-long disruption campaign against the Hive ransomware group that has targeted more than 1,500 victims in over 80 countries around the world, including hospitals, school districts, financial firms, and critical infrastructure." Part of the disruption included the FBI's penetration of Hive's computer networks, capturing its decryption keys and providing them to victims to unlock affected systems and avoid payment of $130 million in demanded ransom. The DOJ stated that the group received over $100 million through its "double-extortion model of attack" of exfiltrating or stealing sensitive data before encrypting the victim's systems, through the use of a ransomware-as-a-service (RaaS) model. Among the methods used by the attackers to gain access to the victim's systems were phishing schemes and emails with malicious attachments.

One takeaway from this announcement is the importance of implementing recognized security practices that are intended to address and prevent the top cyber threats against the healthcare system. This includes having in place a robust security program, including HIPAA Security Rule policies and procedures, implemented practices, ongoing monitoring, and effective training initiatives that address security best practices and avoidance of ransomware attacks and phishing and email schemes.

If you need assistance with your HIPAA compliance program, an OCR investigation, or a data breach incident, please contact:
Lani M. Dornfeld, CHPC | 973.403.3136 | ldornfeld@bracheichler.com