Mail Scam Targeting Healthcare Executives Claims Ties to Ransomware

Source: FBI

The Department of Health and Human Services joins the Federal Bureau of Investigation (FBI) in alerting the Healthcare and Public Health Sector to an ongoing threat targeting sector executives. Today, the FBI issued a cybersecurity alert highlighting a new mail scam that involves fraudulent letters sent by unidentified criminal actors, who claim to be associated with the "BianLian Group," a notorious ransomware organization. The letters are marked as "Time Sensitive Read Immediately" and falsely assert that the BianLian Group has gained unauthorized access to the recipient's organization's network, stealing sensitive data files. The scammers threaten to release this stolen data on BianLian's data leak sites unless the victim pays a ransom of between $250,000 and $500,000 via Bitcoin within ten days. The letter further claims that no negotiations will be entertained, adding a sense of urgency to the demand.

Despite the reference to the BianLian ransomware group, the FBI has stated that there is currently no verified connection between these fraudulent letters and the actual BianLian ransomware operation. The scam appears to be an attempt to extort money from organizations using fear tactics and false claims. The letters feature a return address in Boston, Massachusetts, which is part of the fraud's strategy to create an illusion of legitimacy.

To protect against this threat, the FBI recommends that organizations take immediate steps to raise awareness among their corporate executives about the scam. Employees should also be educated on how to identify and respond to ransom threats, ensuring that they don't fall victim to this or similar tactics. Furthermore, organizations are urged to ensure their network defenses are up to date and that they remain vigilant for any signs of malicious activity. If any suspicious activity or ransomware is detected, the FBI encourages organizations to consult their Joint Cybersecurity Awareness Bulletin for guidance on current tactics, techniques, and procedures used by ransomware groups, as well as indicators of compromise.

In the event that an organization falls victim to this scam, the FBI advises reporting the incident to local FBI Field Offices or the Internet Crime Complaint Center to assist in tracking and addressing the crime. As a reminder, organizations must be cautious and proactive in securing their networks and educating their teams to defend against these types of scams. For more information, please refer to the FBI Alert.