Published on *The National Law Review* https://natlawreview.com

Multiple Federal Agencies Jointly Warn of Increased and Imminent Cybercrime Threat to U.S. Hospitals and Healthcare Providers

Article By:

Peter Baldwin

Jason G. Weiss

On October 28, 2020, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI) and the Department of Health and Human Services (HHS) issued a Joint Cybersecurity Advisory warning of "an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers." The agencies collectively warned that "malicious cyber actors are targeting the Healthcare and Public Health (HPH) Sector with Trickbot malware, often leading to ransomware attacks, data theft, and the disruption of healthcare services."

This advisory provides detailed information about Trickbot malware, including indicators of compromise. Specifically, the advisory includes information about the tactics, techniques and procedures used by cybercriminals to infect systems with "Ryuk" ransomware, which frequently has been deployed in connection with nefarious Trojans like Trickbot.

The HPH Sector has long been a prominent and high-value target for malicious cyber attackers. However, in 2020, ransomware attacks against HPH companies have increased both in frequency and severity – with unfortunate results, including, in at least one case, the death of a patient.

The advisory encourages HPH Sector companies to review and update their business continuity plans so that they will be able to continue to execute essential functions in the event of a cyberattack emergency. HPH System administrators who see indicators of a Trickbot network compromise are advised to immediately "take steps to back up and secure sensitive or proprietary data" because of the risk of an "imminent ransomware attack."

The advisory also lists a number of best practices to minimize damage and disruptions from cyberattacks, including:

- Routinely patch operating systems, software and firmware
- Check operating system configurations to optimize the ability to respond to cyberattacks at

both a system-wide and local level

- Change network passwords regularly
- Use multi-factor authentication
- Disable unused remote access ports and monitor remote access logs
- Implement rules to only allow systems to execute programs known and permitted by established security policies
- Regularly audit user accounts with administrative privileges
- Review logs to ensure the legitimacy of new accounts
- Scan for open or listening ports
- Identify critical assets and create offline backups of these systems
- Implement network segmentation
- Update antivirus and anti-malware software

The Joint Advisory is the latest reminder of the ongoing cyberattack threat faced by companies in the HPH Sector. All companies – especially those in the HPH Sector – should carefully review the Joint Advisory and ensure that they are aware of the threat and that they are complying with the recommended best practices and mitigation measures detailed therein.

National Law Review, Volume X, Number 303