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

Warning to Hospitals of Imminent Threat Released by U.S. Government

Article By:

Linn F. Freedman

On October 27, 2020, the FBI and the Department of Homeland Security (DHS) warned the health care industry about “an imminent cybercrime threat to U.S. hospitals and healthcare providers.”

According to the warning, which was shared during a conference call, the government has received “credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers.” The information was being shared with participants so that they can take timely precautions to protect their networks from the threat.

According to KrebsonSecurity, the threat is believed to be stemming from a Russian cybercriminal gang that may be deploying Ryuk ransomware to more than 400 health care facilities in the U.S. It appears that the attack is planned to be coordinated in order to maximize disruption in the health care sector.

Hospitals are urged to confirm that patching has been completed of all known vulnerabilities. Mandiant has released a list of domains and Internet addresses that have been used by Ryuk in the past to assist hospitals with identifying known methods used to infiltrate systems.

Based upon these warnings, hospitals and health care providers may wish to consider prioritizing patching and blacklisting the known domains and Internet addresses used by Ryuk today.

National Law Review, Volume X, Number 303