FBI Warns of Imminent Cybercrime Threat to U.S. Hospitals and Health Care Providers

Anton Janik, Jr.
ajanik@mwlaw.com
(501) 688.8888

10/29/2020

In a Joint Cybersecurity Advisory issued Wednesday, the Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, and the Department of Health and Human Services warned of an imminent ransomware threat to U.S. hospitals and healthcare providers. More than 400 hospitals, clinics and medical facilities across the U.S. are the reported focus of the attack.

The attack uses the Trickbot malware, which has been in use since 2016 and has been updated with a focus on "ease, speed and profitability of victimization." Originally developed as a banking Trojan, this malware harvests users credentials and exfiltrates data, among other techniques, which provide the hackers with additional powerful methods to gain access to sensitive or secure data systems. The linked Advisory provides technical details for your Information Security teams to analyze systems for this Trojan infection.

The Trickbot hackers steal user credentials as part of their network mapping attempts, enabling them to move across systems including mounted drives. The Trickbot malware then deploys the Ryuk ransomware in the targeted systems. Once activated, Ryuk uses AES-256 to encrypt files and an RSA public key to encrypt the AES key. Ryuk then attempts to delete all backup files and automatic backup snapshots made by Windows, in order to prevent the victim from recovering their files through backups rather than paying the ransom. In addition, the hackers attempt to disable security applications running on the affected systems in order to prevent the applications from disabling the ransomware.

Once the systems are encrypted with the ransomware, the RyukReadMe file is placed on the system, and provides one or two email addresses for the victim to contact the hackers using end to end encrypted email. The ransom amount is only provided after email contact is made. The Advisory warns that even after the ransom is paid, encrypted files may not unencrypt.

The Advisory recommends that where indications of a Trickbot network compromise are found, systems administrators should immediately take steps to back up and secure sensitive or proprietary data using the 3-2-1 rule, where three copies of all critical data are retained on at least two different types of media with at least one of them stored offline. The Advisory also provides a series of best practices on securing your networks and for responding to ransomware threats. The agencies do not advise paying ransoms, since paying ransoms does not guarantee that files will be recovered, and may embolden hackers to target further organizations.