COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 24, Number 3. March 07, 2024 Security Checklist: Guard Against New Akira Ransomware

By Jane Anderson

The HHS Health Sector Cybersecurity Coordination Center (HC3) is warning health organizations to take steps to guard against Akira ransomware, which is deployed by "a relatively new ransomware gang that has demonstrated aggressive and capable targeting of the U.S. health sector in its short lifespan."[1]

Akira ransomware—first identified in May 2023—has claimed at least 81 victims, HC3 said in a February analyst note. The ransomware variant is most likely not related to the Akira variant first observed in 2017, but there is research suggesting that the new version of Akira has connections to the now-defunct Conti ransomware gang; since Conti and Akira appear similar in their exploitation approach, the selection of certain types of files and directories for targeting, their choice of application for encryption algorithms and their use of ransom payment addresses, HC3 said.

"Akira leverages many common features for their targeting and operations," HC3 said. "They operate as ransomware-as-a-service (RaaS), which is to say they focus on the ransomware operations, but partner with other cybercriminals for individual attacks and share the extorted fees."