Report on Patient Privacy Volume 22, Number 9. September 07, 2022 Karakurt Ransomware Cybersecurity Checklist

By Jane Anderson

The HSS Health Sector Cybersecurity Coordination Center (HC3) is warning that threats are increasing from the Karakurt ransomware group. This is a relatively new cybercrime group that HC3 said is responsible for at least four attacks involving the U.S. health care and public health sector since June.[1]

The observed attacks affected an assisted living facility, a dental firm, a health care provider and a hospital, HC3 said.

"Karakurt typically conducts scanning, reconnaissance, and collection on its targets for an estimated two-month time span," the HC3 warning said. "The threat actor gains access to files containing patient names, addresses, Social Security numbers, dates of birth, medical history information, medical diagnosis information, treatment information, medical record numbers and health information. The threat actor then threatens to release the information unless a ransom is paid."