Report on Patient Privacy Volume 23, Number 9. September 07, 2023 HC3: Take Steps to Defend Against Rhysida Ransomware

By Jane Anderson

The HHS Sector Cybersecurity Coordination Center (HC3) is warning health care organizations about Rhysida, a new ransomware-as-a-service group that has emerged in the past three months.[1] The Rhysida ransomware gang claimed responsibility on Aug. 24 for a cyberattack on Prospect Medical Holdings, leading to shutdowns of hospital services across five states.[2]

Rhysida drops ransomware via phishing attacks and Cobalt Strike to breach targets' networks, and then the group threatens to publicly distribute the exfiltrated data if the ransom is not paid. The ransomware also leaves PDF notes on the affected folders, instructing the victims to contact the group via its portal and pay in Bitcoin.

Victims of the group are distributed across Western Europe, North and South America and Australia, according to HC3, which notes that "they primarily attack education, government, manufacturing, and technology and managed service provider sectors; however, there has been recent attacks against the Healthcare and Public Health (HPH) sector."