COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 23, Number 2. February 09, 2023 HHS Warns of New Ransomware Threats, AI-Fueled Phishing Schemes

By Jane Anderson

The U.S. health care sector continues to be targeted aggressively by ransomware operators, with two sophisticated threats—Royal and BlackCat ransomware—gaining in prominence, the HHS Health Sector Cybersecurity Coordination Center (HC3) warned.[1]

At the same time, HC3 said, a third threat—the pro-Russian hacktivist group KillNet—has attacked at least one health care organization in the United States. Plus, HC3 warned, malware is becoming more sophisticated, and artificial intelligence (AI) is expected to accelerate that development.

Those behind Royal, which surpassed Lockbit late in 2022 to become the most notorious ransomware, appear to be a private group without any affiliates, HC3 said. Its motivation is financial, and ransom demands range from $250,000 to more than $2 million.

Royal attacks start in various ways, including phishing campaigns and using common cyber threat loaders such as BATLOADER and QBot, HC3 said. The ransomware employs a "unique approach to evade anti-ransomware defenses," HC3 said.

For example, Royal has used Google Ads in a campaign to blend in with normal ad traffic. This makes malicious downloads appear authentic by hosting fake installer files on legitimate-looking software download sites or using contact forms located on an organization's website to distribute phishing links, HC3 said.