COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 21, Number 8. August 12, 2021 HHS: Conti Takes Ransomware to New Level; No Easy Decryption, Beware Triple Extortion

By Jane Anderson

The Conti ransomware strain poses a significant and growing threat to health care organizations in the United States, and entities should take specific steps now—including increased phishing training and other security measures—to guard against attacks, the federal government is warning.

"Conti is so aggressive that [it] managed to get on the radar of law enforcement earlier this year," according to a federal cybersecurity expert who spoke about Conti during the first in a series of briefings sponsored by the HHS Office of Information Security and Health Sector Cybersecurity Coordination Center, also known as HC3.[1]

As in the past, bad actors using Conti increasingly are targeting the health care sector, in part because it is a rich source of valuable data and organizations' defenses can be fragmented and less effective. In 2020, Conti was the second-most used ransomware to target health care, said the official, who HC3 would not identify to *RPP*. Between February and June of this year, there were 207 gigabytes of leaked data online from Conti attacks, he said.

More than 120 U.S. entities had their data published on a Conti "news" website, according to data compiled in February. Canada and European Union countries also were affected, while Russia and China were spared.

Traditional ransomware tactics, which involve penetrating a system, encrypting it, dropping the ransom note and demanding payment, have proliferated since the advent of Bitcoin in 2008, but Conti takes ransomware further, the HC3 official said.