Philadelphia-area health system says it ‘isolated’ a malware attack

By Sean Lyngaas

Published: 2020-06-19 · Archived: 2026-04-05 14:15:54 UTC

A “malware attack” has hit computer systems at Crozer-Keystone Health System, a large health care provider in the Philadelphia suburbs, a spokesman for the organization said Friday.

“After quickly identifying a recent malware attack, the Crozer-Keystone information technology team took immediate action and began remediating impacted systems,” Crozer-Keystone’s Rich Leonowitz said in an emailed statement.

Crozer-Keystone owns four hospitals and four outpatient centers in Delaware County, Pennsylvania, according to its website. It was not immediately clear how, if at all, the cybersecurity incident impacted those facilities. Leonowitz declined to answer questions on the matter.

“Having isolated the intrusion, we took necessary systems offline to prevent further risk,” Leonowitz’s statement continued. “We completed this work in collaboration with cybersecurity professionals across our health care system and are currently conducting a full investigation of the issue.”

A set of hackers behind the NetWalker ransomware claimed responsibility for the attack. On their victim-shaming website, the hackers shared screenshots that they claimed were encrypted files belonging to Crozer-Keystone. A countdown clock on the site threatens to publicly dump the data in six days unless the hackers are paid a ransom. The dual threat of extorting organizations and dumping data is an increasingly common tactic from ransomware perpetrators.

A sector under stress

It’s just the latest cybersecurity incident to hit the health care sector during the novel coronavirus pandemic. The IT systems at the Czech Republic’s second biggest hospital suffered a cyberattack in March. There have also been ransomware attacks on pharmaceutical and biotech firms helping respond to the coronavirus.

“With ransomware becoming a public health threat to health care systems overburdened during COVID-19, it should be treated as such,” said Beau Woods, a cyber safety innovation fellow at the Atlantic Council.

The hackers behind NetWalker are relatively new to the ransomware scene, but “have been very innovative during their short operational period,” said Allan Liska, a threat intelligence analyst at security company Recorded Future.

“Some of the NetWalker groups have been particularly aggressive in targeting health care providers and they appear to be successful at extracting ransom from these targets as very few have made it to their extortion site,” Liska added.

In March, a NetWalker ransomware attack temporarily disabled the website of a public health agency in Illinois that was updating residents on the spread of coronavirus.
