Ransomware forces 3 hospitals to turn away all but the most critical patients

Enlarge / Emergency rooms like this one at Fort Belvoir Community Hospital may need to transfer patients once they stabilize.

reader comments

122 with 83 posters participating

Share this story

Ten hospitals—three in Alabama and seven in Australia—have been hit with paralyzing ransomware attacks that are affecting their ability to take new patients, it was widely reported on Tuesday.

All three hospitals that make up the DCH Health System in Alabama were closed to new patients on Tuesday as officials there coped with an attack that paralyzed the health network's computer system. The hospitals—DCH Regional Medical Center in Tuscaloosa, Northport Medical Center, and Fayette Medical Center—are turning away "all but the most critical new patients" at the time this post was going live. Local ambulances were being instructed to take patients to other hospitals when possible. Patients coming to DCH emergency rooms faced the possibility of being transferred to another hospital once they were stabilized.

"A criminal is limiting our ability to use our computer systems in exchange for an as-yet unknown payment," DCH representatives wrote in a release. "Our hospitals have

implemented our emergency procedures to ensure safe and efficient operations in the event technology dependent on computers is not available."

Details about the specific strain of malware weren't immediately available. Typically, the malware encrypts production and backup hard drives used to store data and run computer systems. Victims can only receive the decryption key needed to restore systems after paying a ransom, usually using bitcoin or another cryptocurrency. In some cases, it's possible to decrypt data without paying the ransom. In other cases, it's impossible.

Down under

At least seven hospitals in Australia, meanwhile, were also feeling the effects of a ransomware attack that struck on Monday. The hospitals in Gippsland and southwest Victoria said they were rescheduling some patient services as they responded to a "cyber health incident."

"The cyber incident, which was uncovered on Monday, has blocked access to several systems by the infiltration of ransomware, including financial management," hospital officials said. "Hospitals have isolated and disconnected a number of systems… to quarantine the infection."

Hospital officials said they're working with police and the Australian Cyber Security Center to manage the incident. According to news reports, hospital computer systems remained locked down at seven hospitals on Tuesday more than 24 hours after the attack struck. An official said it would take weeks to secure and restore damaged networks. The official said there was no indication that patient records had been accessed.

There was no immediate indication that the attacks in Alabama and Australia were related. One of the most memorable times

hospitals were widely reported to be hamstrung by ransomware attacks was in the wake of the WannaCry ransom worm outbreak in May 2017 and, to a lesser extent, the NotPetya attack that followed two months later.

https://arstechnica.com/?p=1577895