Hospitals that are turning away patients reportedly pay ransomware attackers

reader comments

63 with 47 posters participating

Share this story

Three Alabama hospitals have paid a ransomware demand to the criminals who waged a crippling malware attack that’s forcing the hospitals to turn away all but the most critical patients, the Tuscaloosa News reported.

As reported last Tuesday, ransomware shut down the hospitals’ computer systems and prevented staff from following many normal procedures. Officials have been diverting non-critical patients to nearby hospitals and have warned that emergency patients may also be relocated once they are stabilized. An updated posted on Saturday said the diversion procedure remained in place. All three hospitals are part of the DCH health system in Alabama.

Over the weekend, the Tuscaloosa News said DCH officials made a payment to the people responsible for the ransomware attack. The report didn’t say how much officials paid. Saturday’s statement from DCH officials said they have obtained a decryption key but didn’t say how they obtained it.

The statement read in part:

> *In collaboration with law enforcement and independent IT*

> *security experts, we have begun a methodical process of system restoration. We have been using our own DCH backup files to rebuild certain system components, and we have obtained a decryption key from the attacker to restore access to locked systems.*
>
> *We have successfully completed a test decryption of multiple servers, and we are now executing a sequential plan to decrypt, test, and bring systems online one-by-one. This will be a deliberate progression that will prioritize primary operating systems and essential functions for emergency care. DCH has thousands of computer devices in its network, so this process will take time.*
>
> *We cannot provide a specific timetable at this time, but our teams continue to work around the clock to restore normal hospital operations, as we incrementally bring system components back online across our medical centers. This will require a time-intensive process to complete, as we will continue testing and confirming secure operations as we go.*

DCH representatives didn't respond to an email seeking details and comment for this post.

To pay or not to pay

Law enforcement officials and security professionals generally discourage ransomware payments because such payments encourage more attacks, and there is no guarantee the criminals will produce the key as promised. And even when criminals do produce a key, sometimes the malware can permanently destroy some of the encrypted data. According to a FAQ published by DCH, the strain of ransomware that hit the hospitals is known as Ryuk, which specializes in burrowing deep into infected networks to exact big payments.

"Ryuk is particularly nasty as the code contains bugs that

causes it to damage about one in every eight files that it encrypts," Brett Callow, a spokesman with security firm Emsisoft, told Ars. "So there is almost always data loss in these cases even when the ransom is paid."

Emsisoft provides free tools it says can often decrypt data that's hit by ransomware. But even when it's successful against Ryuk, those tools don't enable corrupted files to be recovered.

The darker side of not paying ransoms is this: often, organizations hit by ransomware end up paying much higher costs when they choose to rebuff the demands. Instead, they attempt to rebuild crippled networks on their own. The city of Baltimore, for example recently paid more than $18 million to restore its ransomware-crippled network. The criminals in that attack had demanded $70,000, but both city and FBI officials discouraged the payment.

The rise of ransomware over the past five years underscores the importance of having a robust and reliable backup system that IT personnel can use in the event a ransomware attack or some other serious event wipes out data. As it turns out, backup regimens are often not as robust as they should be, and even when they are, restoring networks solely from backups can still be costly and time-consuming.

https://arstechnica.com/?p=1581299