Locky Ransomware Strain Led Kentucky Hospital to an “Internal State of Emergency”

Archived: 2026-04-06 15:46:53 UTC

A red marquee bannered on the homepage of the Methodist Hospital in Henderson, Kentucky announced a cyberattack that successfully penetrated their networks, prompting it to operate under an “internal state of emergency”. The advisory said, “*Methodist Hospital is currently working in an Internal State of Emergency due to a Computer Virus that has limited our use of electronic web based services. We are currently working to resolve this issue, until then we will have limited access to web based services and electronic communications.*”

The incident involved a ransomware attack that hit the hospital’s computer systems and hostaged files by way of encrypting and rendering these useless unless a ransom gets paid to obtain a corresponding decrypt key.

[Read: How ransomware worksnews- cybercrime-and-digital-threats**]**

According to Methodist Hospital Information systems director Jamie Reid, the malware in question belonged to the Locky strain of crypto-ransomware, which is capable of encrypting valuable files like documents and images on the infected system before deleting the original files. This means that a victim can only regain access to the data either by paying the demanded ransom, or by accessing backups outside the infected network. It was then reported that the attackers demanded four bitcoins for the key, an amount totaling USD $1,600.

In late Februarynews- cybercrime-and-digital-threats, Locky was found infiltrating systems through a malicious macro found in a Word document. The ransomware strain gets delivered into a victim’s system through email masquerading as an invoice with an attached Word document laced with malicious macros. Such is the case with the Methodist Hospital attack, wherein recipients of the malicious email downloaded and opened a malicious attachment.

[Read: Locky, a new crypto-ransomware type discoverednews- cybercrime-and-digital-threats**]**

According to Reid, the ransomware succeeded in expanding its reach from its initial infection to several systems found in the network. The hospital reacted by shutting down all of its desktop computers, before turning them

back online, one machine after another to check for infection—a process that caused the hospital to temporarily process everything on paper.

David Park, attorney for the Methodist Hospital said, "*We have a pretty robust emergency response system that we developed quite a few years ago, and it struck us that as everyone's talking about the computer problem at the hospital maybe we ought to just treat this like a tornado hit, because we essentially shut our system down and reopened on a computer-by-computer basis.*"

This incident happened barely a month after reports of a similar ransomware attack on another medical institution surfaced. In February 2015, the networks of the Hollywood Presbyterian Medical Centernews article were paralyzed by the same tactic, disrupting hospital operations. This led the institution to pay a ransom that amounted to $17,000 in bitcoins.

However, other means have also been devised by cybercriminals to profit from attacks on the healthcare industry. A recently-reported data breach involving cancer treatment center 21st Century Oncology Holdingsnews-cybercrime-and-digital-threats exposed the information of over 2 million patients. A separate incident involving a phishing attack on research and treatment facility City of Hopenews article has led to the unauthorized access of an employee email account containing protected health information such as patient names, medical record numbers, dates of birth, addresses, and other patient and clinical information.

With that said, given the difference of attack strategies employed in these mentioned incidents, it goes to show that attacks on the healthcare industry show no signs of slowing down. The numbers back it up; according to the recorded data breach incidents in 2015, healthcare was identified to be the most affected industry.

This can be explained by the fact that the healthcare industry houses repositories of profitable types of information that can easily be used to stage other attacks, such as identity theft and even blackmail and other extortion schemes. The number of incidents that involve the theft of medical data shows that these types of data aren't as secure, making it an even more ideal target.

[Read: Why is the healthcare industry an ideal target?news article**]**

As of this writing, the hospital's officials have shared a report to a local TV station that the incident has already been handled and that its internal digital systems are now "up and runningnews article". While the investigation is ongoing and no further details have been divulged, it was noted that no ransom was paid and patient information wasn't compromised. That said, COO David Part shared that currently, with the main network still in downtime, a back-up system has been activated and no operation disruption is being experienced.

HIDE

Like it? Add this infographic to your site:

1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.
