

# Hollywood hospital becomes ransomware victim

By Charlie Osborne

Published: 2016-02-15 · Archived: 2026-04-05 21:53:36 UTC



An example of a ransomware-locked system screen.

A cyberattack launched against the Hollywood Presbyterian Medical Center has forced staff to declare an "internal emergency" and left employees unable to access patient files.

[According to NBC](#), the Southern California hospital has been left unable to practice its usual day-to-day operations. The hospital's president and CEO Allen Stefanek said "significant IT issues" were discovered last week, leading to emergency measures including calling for the assistance of the FBI, Los Angeles Police Department (LAPD) and cyberforensics experts.

An unnamed doctor at the hospital said that the system was hacked and "held for ransom," which suggests ransomware was put into play. This [particular breed of malware](#), usually spread through phishing campaigns and malicious downloads, installs itself on victim machines in order to encrypt system files.

Once a PC is infected, the system is locked and a warning message comes into play, telling the user that they have a time limit before their files are lost forever, and in order to decrypt these files, they must pay a fee -- usually in a cryptocurrency such as Bitcoin to make tracking cybercriminals difficult.

It is not currently known if patient or employee information was compromised in the attack, but if ransomware was the core source of the attack, the main reason for the cyberattack would have been to secure the ransom payment rather than steal data belonging to the hospital.

Stefanek admitted the emergency section of the hospital has been "sporadically impacted" since Friday, and the doctor said email services, in particular, were taken down. As medical records including patient details, X-rays, CT scans and lab work could not be accessed, this has made the situation very dangerous for patients.

As a result, a number of patients have not been able to receive treatment and some have been transported to other hospitals.

Medical staff have been relying on fax machines and telephones as the week-long outage continues to wreak havoc, which had led to a decrease in efficiency and an inability, in some cases, to safely help patients.

Fox [asked for additional details](#) of the cyberattack from computer forensics expert Eric Robi, who said the ransom was extremely high in this case and may have been for up to 9,000 Bitcoin, or the equivalent of approximately \$3.6 million.

This type of ransom is far higher than what attackers usually demand -- especially as ransomware is often found on individual PCs having been spread through phishing campaigns -- but the high-profile of the hospital and urgency to unlock files intact may have led to such a steep demand.

At the Kaspersky Security Analyst Summit (SAS) in Tenerife, Spain, security expert Sergey Lozhkin demonstrated how [easy it is to compromise medical networks](#) and equipment through simple, elegant hacks -- made possible through almost universal poor security, unprotected Wi-Fi networks and outdated firmware.

#### **Read on: Top picks**

- [Port Fail VPN security flaw exposes your true IP address](#)
- [Dealers hit Volkswagen with class action lawsuits over emissions scandal](#)
- [Bug bounties: Which companies offer researchers cash?](#)
- [Your business has suffered a data breach. Now what?](#)

---

Source: <https://www.zdnet.com/article/hollywood-hospital-becomes-ransomware-victim/>