

Hive ransomware shuts down California health care organization

By Jonathan Greig

Published: 2023-01-17 · Archived: 2026-04-06 00:35:21 UTC

Partnership HealthPlan of California, a nonprofit that helps hundreds of thousands of people access health care in California, is in the midst of being attacked by the Hive ransomware group.

The organization is one of the largest Medi-Cal Managed Care Plan providers in Northern California and serves more than 610,000 Medi-Cal beneficiaries in 14 northern California counties.

It is unclear when the attack began and Partnership HealthPlan of California is currently unable to respond to requests for comment, but local California newspaper [The Press Democrat](#) was the first to report on March 24 that the organization was facing technical issues.

On its website, the organization said it “began experiencing technical difficulties, resulting in a disruption to certain computer systems.” It has hired cybersecurity experts to deal with the disruption and restore its systems.

They urged people and hospitals to contact them by email but said not to include any personal information in the email.

“At this time, PHC is unable to receive or process Treatment Authorization Requests (TAR). For procedures scheduled within the next two (2) weeks, inpatient admission or for urgent services, please proceed with providing the necessary treatment(s) and the appropriate TARs can be completed retroactively,” the organization said on its website, which is down aside from a screen showing this message.



Image: Partnership HealthPlan of California

Emsisoft threat analyst Brett Callow shared a screenshot of the Hive ransomware page where the group says it has attacked Partnership HealthPlan of California and stolen the personal information of more than 850,000 people.

The group also claims to have stolen 400 GB from the organization's servers.

The ransomware gang said it encrypted the organization's systems on March 19 but only added them to the leak site on March 29.

The FBI [spotlighted the Hive ransomware group](#) in August 2021 after their members ransomed dozens of healthcare organizations last year.

In 2021, Hive attacked [at least 28 healthcare organizations](#), including Memorial Health System in Ohio and West Virginia, which was [hit with a ransomware attack on August 15](#). Callow noted that at least four US hospitals have been hit with ransomware this year.

Memorial Health System CEO Scott Cantley [said in a statement](#) at the time that staff at three hospitals -- Marietta Memorial, Selby, and Sistersville General Hospital -- were forced to use paper charts.

All urgent surgical cases and radiology exams [were canceled](#) because of the attack. Memorial Health System Emergency Departments were forced to go on diversion due to the attack.

Marietta Memorial Hospital agreed only to keep taking patients suffering from strokes and trauma incidents. Anyone else in need of help simply had to be transported to other hospitals.

The hospital system [ended up paying a ransom](#) to Hive.

"Unfortunately, many health care organizations are confronting the impacts of an evolving cyber threat landscape," Cantley said at the time. In February, a team of South Korean researchers [published an academic paper](#) on ways organizations can recover files encrypted by the Hive ransomware without paying the attackers for the decryption key.

Get more insights with the

Recorded Future

Intelligence Cloud.

[Learn more.](#)

 Recorded Future®

Know what matters.

Act first.

Get started



No previous article

No new articles



[Jonathan Greig](#)

is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.

Source: <https://therecord.media/hive-ransomware-shuts-down-california-health-care-organization/>