

# Ransomware gang posts breast cancer patients' clinical photographs

By Alexander Martin

Published: 2023-03-06 · Archived: 2026-04-05 13:17:59 UTC

The ALPHV ransomware group, also known as BlackCat, is attempting to extort a healthcare network in Pennsylvania by publishing photographs of breast cancer patients.

These clinical images, used by Lehigh Valley Health Network as part of radiotherapy to tackle malignant cells, were described as “nude photos” on the criminals’ site.

Lehigh Valley Health Network disclosed on February 20 that it had been attacked by the BlackCat gang, which it described as linked to Russia, and stated that it would not pay a ransom.

“Based on our initial analysis, the attack was on the network supporting one physician practice located in Lackawanna County. We take this very seriously and protecting the data security and privacy of our patients, physicians and staff is critical,” said the network’s president and chief executive, Brian Nester.

Nester added that the incident involved “a computer system used for clinically appropriate patient images for radiation oncology treatment and other sensitive information.”

At the time of the original statement, Nester said Lehigh Valley Health Network’s services — including a cancer institute and a children’s hospital — were not affected.

However the network’s website is currently inaccessible. The Record was unable to contact the network for further comment following its listing on the ALPHV [.onion](#) website.

Onlookers have been revolted by the attempt to leverage the sensitivities around cancer treatment and intimate images to extort the organization.

Max Smeets, an academic at ETH Zurich — a public research university — and the director of the European Cyber Conflict Research Initiative, [wrote](#): “This makes me so angry. I hope these barbarians will be held accountable for their heinous actions.”

"A new low. This is sickening," [wrote](#) malware analyst Ryan Chapman, while Nicholas Carroll, a cybersecurity professional, [said](#) the gang was “trying to set new standards in despicable.”

ALPHV itself celebrated the attack and the attention it brought.

“Our blog is followed by a lot of world media, the case will be widely publicized and will cause significant damage to your business. Your time is running out. We are ready to unleash our full power on you!”

Numerous healthcare organizations have been attacked by ransomware gangs in recent months. The criminal industry persists because of victims who pay, sometimes because their businesses face an existential threat, and sometimes to avoid the negative publicity.

Medibank, one of Australia's largest health insurance providers, stated last November that it would not be making a [ransom payment](#) after hackers gained access to the data of 9.7 million current and former customers, including 1.8 million international customers living abroad.

The information included sensitive healthcare claims data for around 480,000 individuals, including information about drug addiction treatments and abortions. Outrage at the attack prompted the government to [consider banning](#) ransomware payments in a bid to undermine the industry.

Back in January, the hospital technology giant [NextGen Healthcare](#) said it was responding to a cyberattack after ALPHV added the company to its list of victims.

 Recorded Future®

Know what matters.

Act first.

Get started



No previous article

No new articles



[Alexander Martin](#)

is the UK Editor for Recorded Future News. He was previously a technology reporter for Sky News and a fellow at the European Cyber Conflict Research Initiative, now Virtual Routes. He can be reached securely using Signal on: AlexanderMartin.79

---

Source: <https://therecord.media/ransomware-lehigh-valley-alphv-black-cat>