UnitedHealth subsidiary Optum hack linked to BlackCat ransomware

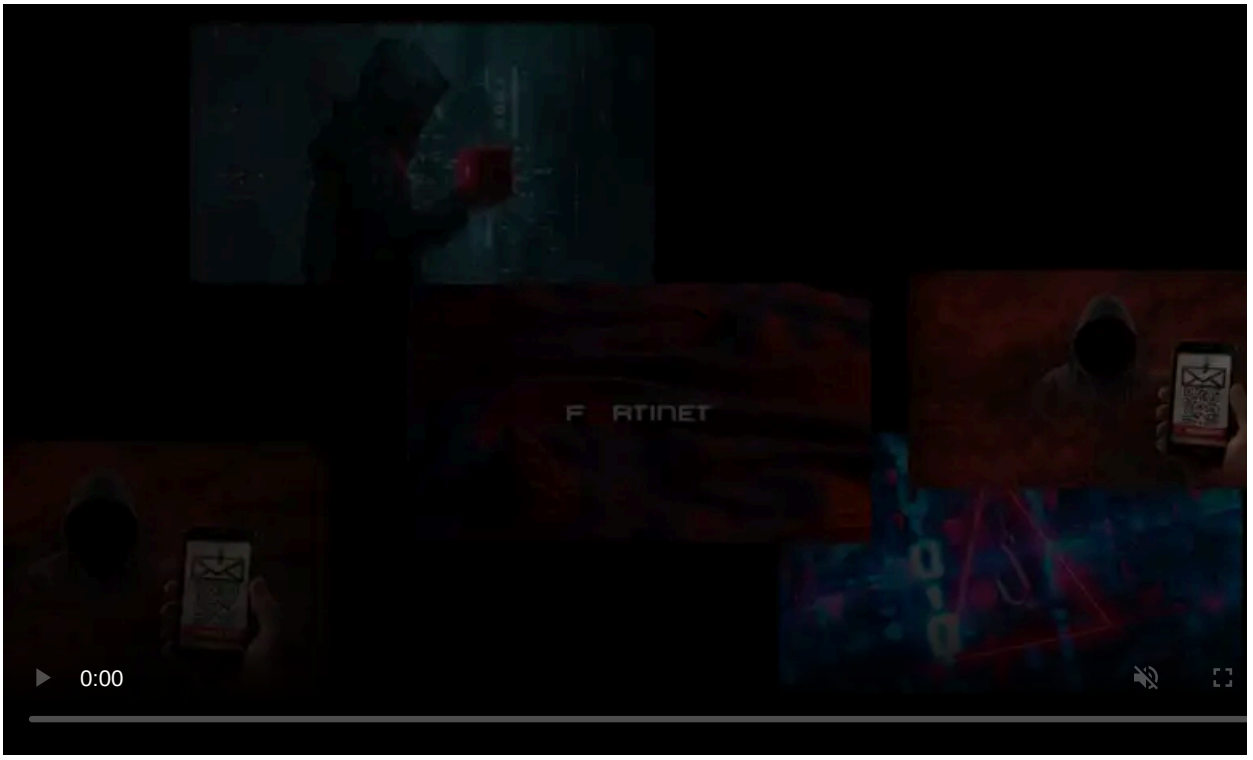
By Sergiu Gatlan

Published: 2024-02-27 · Archived: 2026-04-06 03:10:58 UTC

A cyberattack on UnitedHealth Group subsidiary Optum that led to an ongoing outage impacting the Change Healthcare payment exchange platform was linked to the BlackCat ransomware group by sources familiar with the investigation.

Change Healthcare warned customers on Wednesday that some of its services are offline because of a cybersecurity incident. One day later, UnitedHealth Group said in an SEC 8-K filing that the cyberattack was coordinated by suspected "nation-state" hackers who gained access to Change Healthcare's IT systems.

The Change Healthcare shutdown has led to widespread billing outages since the platform is widely used across the U.S. healthcare system by electronic health record (EHR), payment processing, care coordination, and data analytics systems in hospitals, clinics, and pharmacies.


F RTINET
0:00

Since then, Optum has been providing daily incident updates on a dedicated status page, warning that Change Healthcare's systems are still offline to prevent further impact and contain the breach, with the outage currently impacting most services.

"We have a high-level of confidence that Optum, UnitedHealthcare and UnitedHealth Group systems have not been affected by this issue," Optum says.

"We are working on multiple approaches to restore the impacted environment and will not take any shortcuts or take any additional risk as we bring our systems back online."

BlackCat links

Since the attack hit its systems, ChangeHealthcare has been conducting Zoom calls with partners in the healthcare industry to provide updates about the cyberattack.

One of those involved in these calls told BleepingComputer that the attack was linked to the BlackCat (ALPHV) ransomware gang by forensic experts involved in the incident response (Reuters first reported the Blackcat link on Monday).

Another source told BleepingComputer on Friday that one of the indicators of compromise is a critical ScreenConnect auth bypass flaw (CVE-2024-1709) actively exploited in attacks to deploy ransomware on unpatched servers.

BleepingComputer has not been able to independently confirm the sources' claims. At the time of this publication, BlackCat had yet to claim the attack on Change Healthcare, indicating that they may still be in the process of trying to extort a ransom.

UnitedHealth Group VP Tyler Mason did not confirm whether BlackCat was responsible for the attack but said that 90% of affected pharmacies had implemented new electronic claim processes to address Change Healthcare issues.

"We estimate more than 90% of the nation’s 70,000+ pharmacies have modified electronic claim processing to mitigate impacts from the Change Healthcare cyber security issue; the remainder have offline processing workarounds," Mason said.

"Both Optum Rx and UnitedHealthcare are seeing minimal reports, including less than 100 out of more than 65 million PBM members not being able to get their prescriptions. Those patients have been immediately escalated and we have no reports of continuity of care issues."

United Health Group (UHG) is a health insurance company with a presence across all 50 U.S. states that has contracts with more than 1.6 million physicians and care professionals, as well as 8,000 hospitals and other care facilities.

UHG employs 440,000 people worldwide and is the world's largest healthcare company by revenue ($324.2 billion in 2022).

Optum Solutions, its subsidiary, operates the Change Healthcare platform, the largest payment exchange platform connecting doctors, pharmacies, healthcare providers, and patients in the U.S. healthcare system.

A BlackCat representative did not respond to BleepingComputer's request for comment before this article was published.

Who is BlackCat/ALPHV?

BlackCat surfaced in November 2021 as a suspected rebrand of the DarkSide and BlackMatter ransomware operations.

DarkSide quickly gained worldwide notoriety after the Colonial Pipeline attack, which resulted in extensive investigations by law enforcement agencies around the globe and the operation having to go through two more rebrands.

The FBI linked BlackCat to over 60 breaches during its first four months of activity between November 2021 and March 2022. It also estimates that BlackCat has raked in at least $300 million in ransom payments from more than 1,000 victims until September 2023.

The gang's operations were disrupted in December, with the FBI temporarily taking down its Tor negotiation and leak sites after hacking its servers and creating a decryption tool using keys collected during the months-long intrusion.

BlackCat has since "unseized" their leak site using private keys they still owned and is now operating a new Tor leak site that the FBI has yet to take down.

While UnitedHealth Group's SEC filing states that a nation-state threat actor is behind the attack, BlackCat has not been publicly linked to any foreign government agencies.

The U.S. State Department is offering rewards of up to $10 million for tips leading to the identification or location of ALPHV gang leaders and $5 million for information on individuals linked to BlackCat ransomware attacks.

Update February 27, 02:59 EST: Added UnitedHealth Group statement.
