Cybercrime as-a-service , Fraud Management & Cybercrime , Healthcare

A Second Gang Shakes Down UnitedHealth Group for Ransom

RansomHub Claims It Has 4TBs of Data Stolen by BlackCat in Change Healthcare Attack

Marianne Kolbasuk McGee (HealthInfoSec) • April 8, 2024

Cybercrime gang RansomHub is demanding that UnitedHealth Group pay a ransom for data BlackCat stole in the Change Healthcare attack. (Image: Getty)

As if things weren't messy enough in the Change Healthcare attack, a second cybercriminal gang - RansomHub - is trying to shake down the company's parent, UnitedHealth Group, and have it pay another ransom for data that an affiliate of ransomware-as-a-service group BlackCat claims to have stolen in February.

See Also: Take Inventory of Your Medical Device Security Risks

Threat intelligence firm SOCRadar in a blog post Monday said RansomHub is threatening to sell "to the highest bidder" 4 terabytes of "highly sensitive data" stolen in the Change Healthcare attack.

UnitedHealth Group had reportedly paid BlackCat, also known as Alphv, a $22 million ransom for a decryptor key and to prevent a data leak in the aftermath of the Feb. 21 attack. The latest ransom demand underscores why cybercriminals cannot be trusted, according to cybersecurity experts.

"Bottom line: This is why companies shouldn't pay demands. It was always a very bad option, and it's now an even worse option," said Brett Callow, a threat analyst at security firm Emsisoft.

Within a month of the attack and ransom demand, a BlackCat affiliate who took credit for the Change Healthcare attack subsequently claimed BlackCat kept all of the ransom payment, rather than sharing the affiliate's cut. For most groups, affiliates receive 70% or 80% of every ransom paid (see: *BlackCat Ransomware Group 'Seizure' Appears to Be Exit Scam*).

But shortly after the affiliate said they were stiffed out of their share of the Change Healthcare ransom, BlackCat's Tor-based data leak site shut down last month, and its web page simply said: "The Federal Bureau of Investigation seized this site as part of a coordinated law enforcement action taken against Alphv/Blackcat ransomware."

While a joint law enforcement operation did seize BlackCat's infrastructure last December and temporarily disrupted the group, law enforcement officials deny taking the operation down a second time in the wake of the Change Healthcare attack, fueling speculation that BlackCat was pulling an exit scam.

Now, in the latest chapter in the saga, RansomHub said on its dark web site: "ALPHV stole the $22 million USD ransom that Change Healthcare and UnitedHealth paid in order to restore their systems and prevent the data leak. However, we have the data, not ALPHV."

The data consists of over 4 terabytes of information that relates to "all Change Healthcare clients that have sensitive data being processed by the company," RansomHub said.

RansomHub claims the stolen Change Healthcare data pertains to "millions" of active U.S. military and Navy personnel, medical and dental records, payment and claims information, patient Social Security numbers and other personal information, insurance records, 3,000-plus source code files for Change Healthcare solutions, "and many more."

UnitedHealth on Monday in a statement to Information Security Media Group said it knows about the RansomHub claims. "We are aware of these reports and continue to work with the authorities," the company said. It declined to make further comment.

Callow at Emsisoft said there are several possibilities about what's going on with the latest RansomHub claims.

"I suspect this is what it seems to be: a scammed affiliate attempting to get paid. That said, there are multiple other options too, including RansomHub being an Alphv rebrand or it being a complete bluff with RansomHub having no data at all," he said.

"As law enforcement ramps up counter-ransomware efforts, it's not unlikely that we'll see more incidents like this, with the criminals scamming each other, scamming victims and trying to create confusion in order to evade sanctions."

Yossi Rachman, senior director of research at security firm Semperis, also said the RansomHub claims could indicate a number of potential scenarios playing out.

"It's possible, just like in most breaches, that Change couldn't secure itself in time to prevent additional breaches exploiting the same or similar attack vectors," he said. "In this case, and since Change became a very lucrative target as it's already shown willingness to pay ransom, the motivation for continuous attacks against Change is exceptionally high."

RansomHub appears to have been established recently - sometime around February 2024, Rachman said.

"It's also possible that affiliates claiming to have been scammed by BlackCat/Alphv started their own alternative ransomware group. This would definitely explain the specific way RansomHub operates its affiliate model, where money arrives at affiliates first and only then 10% of it goes to the actual ransomware group."

RansomHub states it does not allow targeting of North Korea, China, Cuba and the Commonwealth of Independent States. The CIS is a group of nations that were formerly part of the Soviet Union, excluding Georgia and Ukraine - two countries Russia had waged war against, Rachman said.

"To this respect it seems RansomHub is either sponsored, operated by, or working from the Russian Federation or for the benefit of Russian interests," he said.

Previous RansomHub attacks hit targets in the U.S., Brazil and Southeast Asia, in several industries not limited to healthcare, Rachman said.

UnitedHealth Group and its Change Healthcare unit are still working to restore all IT services disrupted by the February attack and are facing more than two dozen proposed class action lawsuits filed in recent days and weeks (see: *Change Healthcare Attack Recovery Woes; Lawsuits Pile Up*).

About the Author

Marianne Kolbasuk McGee

Executive Editor, HealthcareInfoSecurity, ISMG

McGee is executive editor of Information Security Media Group's HealthcareInfoSecurity.com media site. She has about 30 years of IT journalism experience, with a focus on healthcare information technology issues for more than 15 years. Before joining ISMG in 2012, she was a reporter at InformationWeek magazine and news site and played a lead role in the launch of InformationWeek's healthcare IT media site.