BlackCat ransomware turns off servers amid claim they stole $22 million ransom

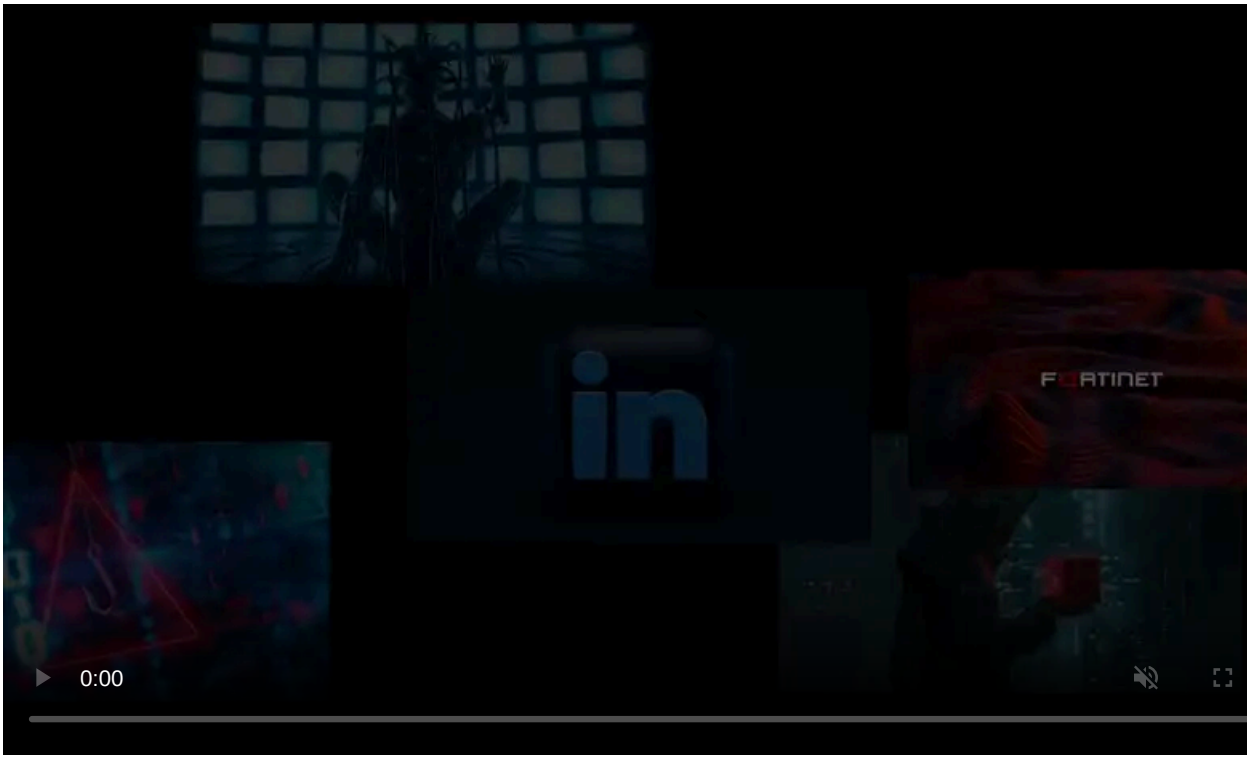
By Ionut Ilascu

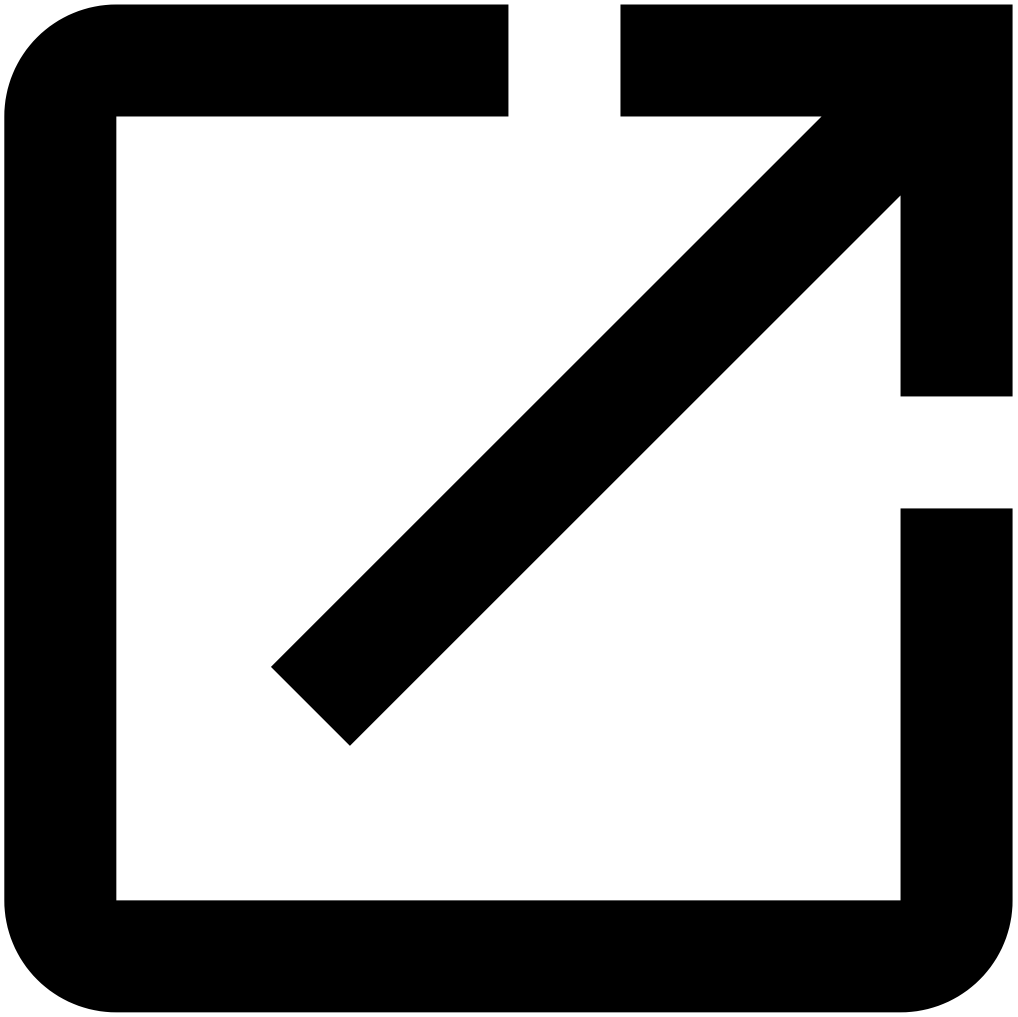
Published: 2024-03-04 · Archived: 2026-04-05 19:37:07 UTC

The ALPHV/BlackCat ransomware gang has shut down its servers amid claims that they scammed the affiliate responsible for the attack on Optum, the operator of the Change Healthcare platform, of $22 million.

While BlackCat's data leak blog has been down since Friday, BleepingComputer had confirmed that negotiation sites were still active over the weekend.

Today, BleepingComputer confirmed the ransomware operations negotiation sites are now shut down as well, indicating a further deliberate take down of the ransomware gang's infrastructure.


0:00



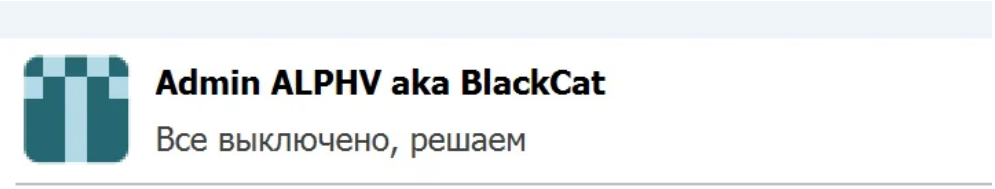
A short status in Russian on the messaging platform the ransomware threat actor uses for communication reads that they decided to turn everything off.

It is unclear if this is an exit scam or an attempt to rebrand the operation under a different name.

Change Healthcare is a payment exchange platform that connects doctors, pharmacies, healthcare providers, and patients in the U.S. healthcare system.

Optum allegedly pays ransom

Earlier today, the Tox messaging platform used by the BlackCat ransomware operator contained a message that does does not provide any details about what the gang plans next: “Все выключено, решаем,” which translates to "Everything is off, we decide."

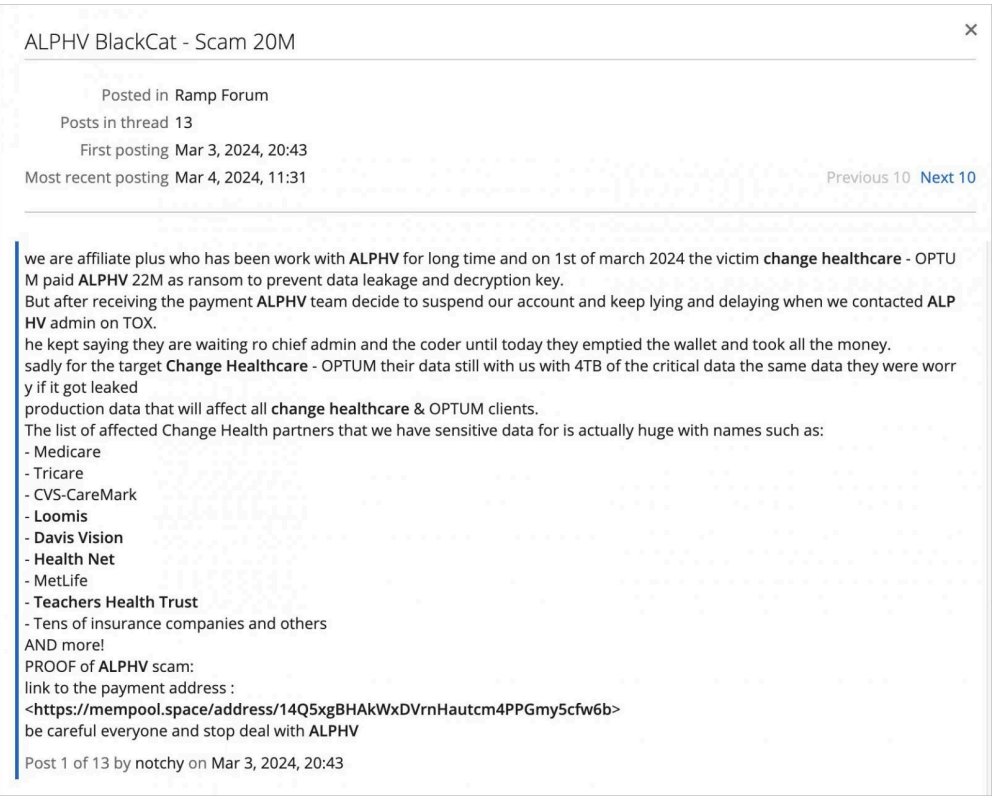


ALPHV decides to turn off servers
source: BleepingComputer

This status message has now been changed to 'GG,' which may mean 'good game.' However, the context of this message is unclear.

This decision may be related to claims from someone describing themselves as a longtime ALPHV/BlackCat affiliate responsible for the attack on Optum, who said that ALPHV banned them from the operation and stole a $22 million ransom allegedly paid by Optum for the Change Healthcare attack.

Dmitry Smilyanets of threat intelligence company Recorded Future shared the message from the alleged ransomware affiliate, which claimed that Optum paid ALPHV/BlackCat a ransom on March 1st to delete the data stolen from the Change Healthcare platform and to receive a decryptor.



ALPHV BlackCat - Scam 20M

Posted in Ramp Forum
Posts in thread 13
First posting Mar 3, 2024, 20:43
Most recent posting Mar 4, 2024, 11:31

Previous 10 Next 10

we are affiliate plus who has been work with **ALPHV** for long time and on 1st of march 2024 the victim **change healthcare** - OPTUM paid **ALPHV** 22M as ransom to prevent data leakage and decryption key.
But after receiving the payment **ALPHV** team decide to suspend our account and keep lying and delaying when we contacted **ALPHV** admin on TOX.
he kept saying they are waiting ro chief admin and the coder until today they emptied the wallet and took all the money.
sadly for the target **Change Healthcare** - OPTUM their data still with us with 4TB of the critical data the same data they were worry if it got leaked
production data that will affect all **change healthcare** & OPTUM clients.
The list of affected Change Health partners that we have sensitive data for is actually huge with names such as:
- Medicare
- Tricare
- CVS-CareMark
- **Loomis**
- **Davis Vision**
- **Health Net**
- MetLife
- **Teachers Health Trust**
- Tens of insurance companies and others
AND more!
PROOF of **ALPHV** scam:
link to the payment address :
<**https://mempool.space/address/14Q5xgBHAkWxDVrnHautcm4PPGmy5cfw6b**>
be careful everyone and stop deal with **ALPHV**

Post 1 of 13 by notchy on Mar 3, 2024, 20:43

Alleged ALPHV affiliate claims they got scammed of the alleged Optum ransom of $22 million
source: Dmitry Smilyanets

Ransomware-as-a-service (RaaS) operations typically work by partnering with external affiliates, who carry out attacks using the operation's encryptors.

Ransoms received from victims are shared between the RaaS administrators and the affiliate responsible for the breach and deploying the ransomware or stealing data.

In this case, it seems that the affiliate that stole data from Change Healthcare got scammed. They claim that after Optum paid a $22 million ransom ALPHV suspended their partner's account and took all the money from the wallet.

Under the username "notchy," the alleged ALPH affiliate says that they still have 4TB of Optum's "critical data," describing it as "production data that will affect all Change Healthcare and Optum clients."

They claim to have data from "tens of insurance companies" and other providers of a range of services from healthcare to cash management, and pharmacies.

To prove their claim, notchy shared a cryptocurrency payment address with a total of nine transactions, an initial incoming transfer of 350 bitcoins (a little over $23 million), and eight outgoing ones.

The address sending the bitcoin has only two transactions, one receiving 350 bitcoins and another sending them to the alleged ALPHV wallet.

BleepingComputer contacted Optum's parent company UnitedHealth Group regarding the claims they paid a ransom payment and was told, "We are focused on the investigation" and that no additional comments are available.

While it is unclear what direction BlackCat is taking, this activity could point to the start of an exit scam, where the ransomware operations steal their affiliates' cryptocurrency and then shut down their operations.

BlackCat is a rebrand of the DarkSide ransomware operation, who also shut down after claiming law enforcement transferred cryptocurrency from their wallets. After the recent law enforcement operation that disrupted BlackCat's servers, it would not be surprising to find that they make a similar claim if they shut down.

From DarkSide to BlackMatter to ALPHV

ALPHV/BlackCat started in 2020 as DarkSide. A year later, the gang attacked the Colonial Pipeline, leading to panic and gas outages in the US.

The ransomware gang lost access to their infrastructure shortly after the attack, claiming their hosting provider blocked access to the servers.

At the time, the gang also said that the funds on their payment server mysteriously disappeared into an unknown account.

The ransomware operation re-emerged a few months later as BlackMatter only to shut down four months later, in November 2021, due to "pressure from the authorities."

The gang resumed operations once more in February 2022 under the ALPHV/BlackCat name and expanded its partnership to English-speaking affiliates.

At the end of last year, the FBI announced that it had breached the ransomware gang's servers, monitored their activity, and obtained private decryption keys that helped more than 400 victims to recover their data for free.

ALPHV restored its infrastructure, though, and continued breaching companies and leaking data from victims that did not pay a ransom.

However, a rebrand may be imminent.
