BlackCat ransomware shuts down in exit scam, blames the "feds"

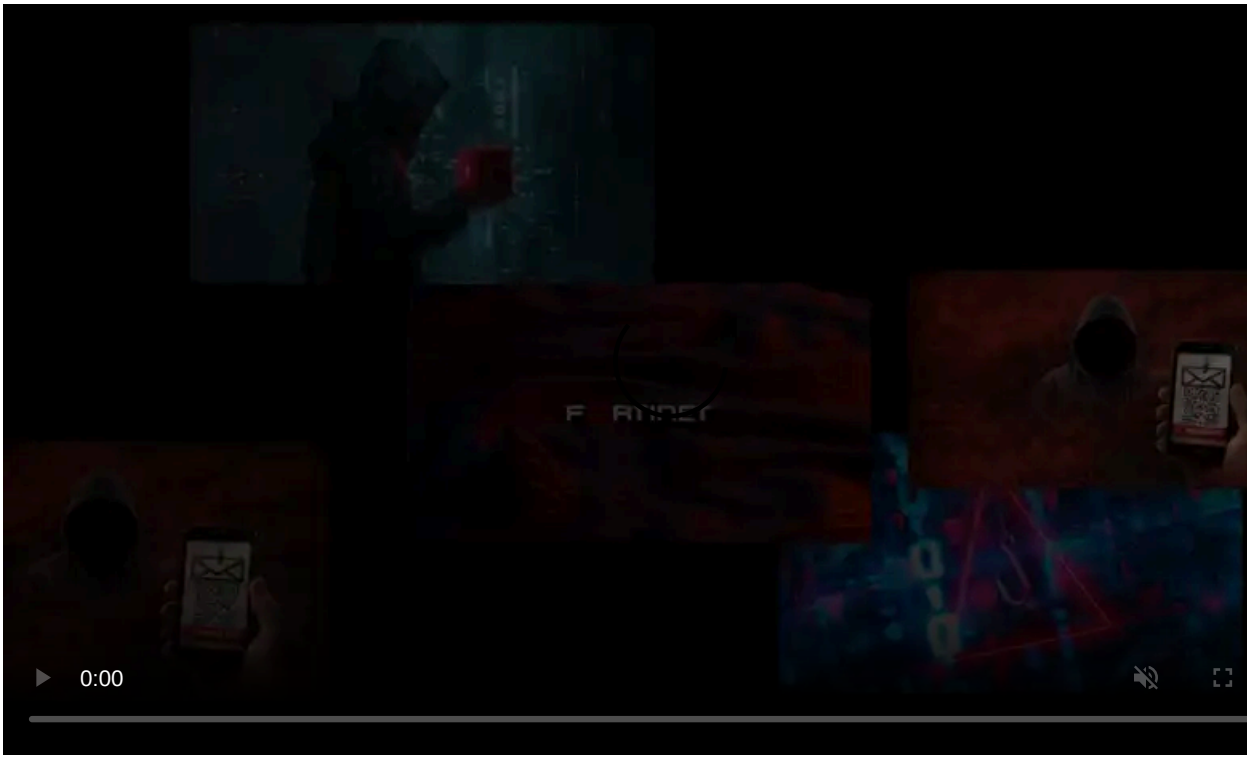
By Ionut Ilascu

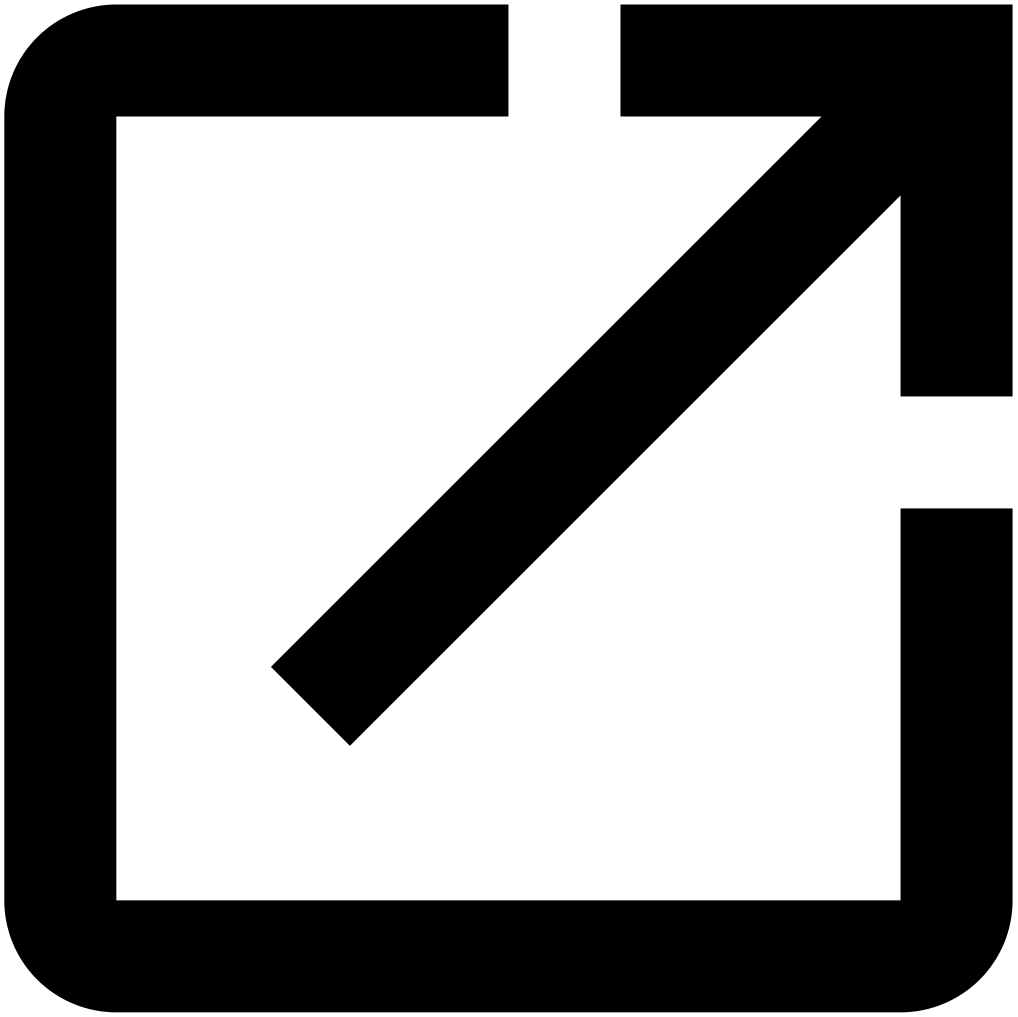
Published: 2024-03-05 · Archived: 2026-04-06 02:08:18 UTC

The BlackCat ransomware gang is pulling an exit scam, trying to shut down and run off with affiliates' money by pretending the FBI seized their site and infrastructure.

The gang announced they are now selling the source code for the malware for the hefty price of $5 million.

On a hacker forum, ALPHV said that they decided "to close the project" because of "the feds," without providing additional details or a clarification.


0:00

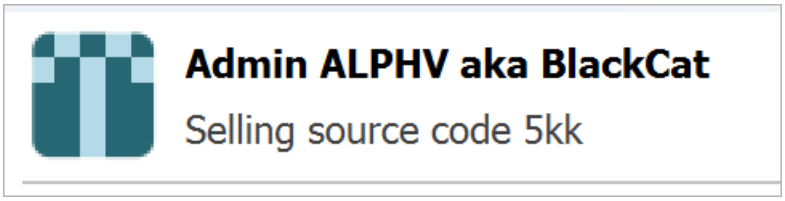


However, a national law enforcement agency listed on the seizure banner confirmed to BleepingComputer that they were not involved in any recent disruption of ALPHV infrastructure.

'The feds screwed us over'

The ransomware gang started the exit-scam operation on Friday, when they took their Tor data leak blog offline. On Monday, they further shut down the negotiation servers, saying that they decided to turn everything off, amid complaints from an affiliate that the operators stole a $20 million Change Healthcare ransom from them."

Yesterday, the gang's status on Tox changed to 'GG' ('good game') - hinting at the end of the operation, and later to "selling source code 5kk," indicating that they wanted $5 million for their malware.

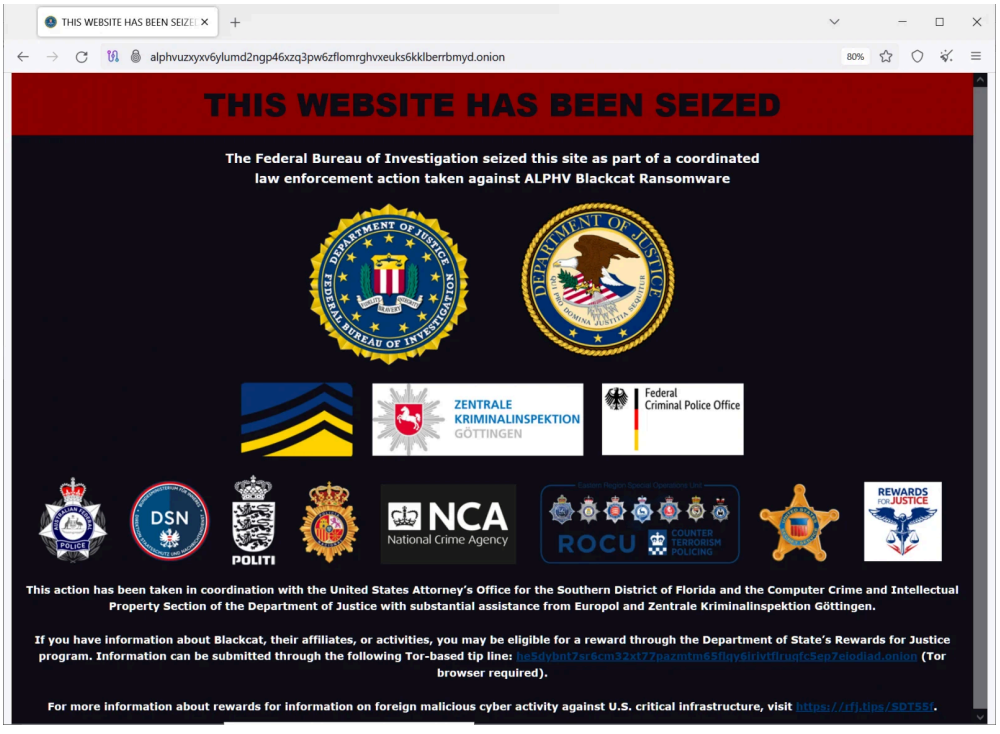


BlackCat ransomware status on Tox messaging platform
source: BleepingComputer

In a message on a hacker forum shared by Recorded Future's Dmitry Smilyanets, the administrators of the operation said that they "decided to completely close the project" and "we can officially declare that the feds screwed us over.

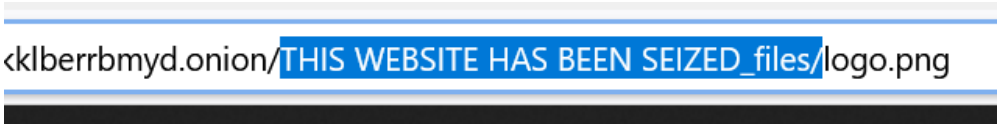
At the time of writing, the ALPHV leak site shows a fake banner announcing that the Federal Bureau of Investigation (FBI) seized the server in a “coordinated law enforcement action taken against ALPHV Blackcat Ransomware.

While the FBI has declined to comment on the seizure notice, Europol and the NCA told BleepingComputer that they are not involved in any recent disruption to ALPHV's infrastructure, even though they are listed on the fake seizure message.



Fake FBI banner on ALPHV ransomware data leak site
source: BleepingComputer

BleepingComputer noticed that the seizure banner image is hosted under a folder named "/THIS WEBSITE HAS BEEN SEIZED_files/," which clearly indicates that the banner was extracted from an archive.



Banner added on ALPHV site
source: BleepingComputer

Ransomware expert Fabian Wosar told BleepingComputer that the ransomware gang simply setup a Python SimpleHTTPServer to serve the fake banner.

"So they simply saved the takedown notice from the old leak site and spun up a Python HTTP server to serve it under their new leak site. Lazy," Fabian Wosar told BleepingComputer.

Additionally, Wosar says that his contacts at Europol an the NCA "declined any sort of involvement" in seizing the ALPHV ransomware site.

Despite NCA's statement and evidence that the banner on the leak site is not the result of law enforcement activity, ALPHV told BleepingComputer that their infrastructure was seized.

Rumors of a possible exit scam from ALPHV started when a longtime ALPHV partner, a so-called "Notchy," claimed that the gang had closed their account and robbed them of a $22 million payment from the ransom allegedly paid by Optum for the Change Healthcare attack.

As proof of their claim, the affiliate shared a cryptocurrency payment address that recorded only one incoming transfer of 350 bitcoins (about $23 million) from a wallet that appears to have been used specifically for this transaction on March 2nd.

After getting the funds, the recipient address that allegedly belongs to ALPHV operators distributed the bitcoins to various wallets in equal transactions of about $3.3 million.

It is worth noting that while the recipient address is now empty, it shows that it received and sent close to $94 million.

With claims from affiliates not getting paid, a sudden shut down of the infrastructure, cutting ties with multiple affiliates, the "GG" message on Tox, announcing that they're selling the malware source code, and especially pretending that the FBI took control of their websites, all this is a cleart indication that ALPHV/BlackCat ransomware administrators are exit scamming.

Who is BlackCat/ALPHV ransomware

The operators of BlackCat have been involved in ransomware since at least 2020, first launching as DarkSide in August 2020 as a ransomware-as-a-service (RaaS) operation.

A RaaS is when core operators develop a ransomware encryptor and negotiation sites and recruit affiliates to use their tools to conduct ransomware attacks and steal data.

After a ransom is paid, the operators split the ransom payment, with affiliates and their teams usually receiving 70-80% of the payment and the operation receiving the rest.

After their widely publicized attack on Colonial Pipeline, the threat actors shut down the DarkSide operation in May 2021 under intense pressure from global law enforcement.

While ransomware gangs were already under scrutiny by law enforcement, the attack on Colonial Pipeline was a tipping point for governments worldwide who began prioritizing targeting these cybercrime operations.

Instead of staying away, the operators launched a new ransomware operation called BlackMatter on July 31st, 2021. However, the cybercriminals quickly shut down again in November 2021 after Emsisoft exploited a weakness to create a decryptor, and servers were seized.

Instead of learning from their mistakes, the ransomware operators returned in November 2021, this time under the name BlackCat or ALPHV.

While the gang's official name is ALPHV, it was not known at the time, so researchers called it BlackCat based on the small icon of a black cat used on every victim's negotiation site.

Since then, the ransomware gang has continuously evolved its extortion tactics, taking the unusual approach of partnering with English-speaking affiliates.

However, last year, the threat actors grew increasingly toxic, working with affiliates who threatened physical harm, posting nude photos from stolen data, and aggressively calling out victims.

With this new extortion strategy, the ransomware gang was firmly planted in the crosshairs of law enforcement.

In December 2023, an international law enforcement operation seized the ransomware gang's Tor negotiation and data leak sites.

The FBI also announced that they had hacked BlackCat's servers and quietly collected information on the cybercriminals while obtaining decryptors to allow victims to recover their files for free.

Instead of shutting down, the ransomware gang continued their activities, vowing to retaliate against the US government by attacking critical infrastructure.

Never learning from their past mistakes, the ransomware gang once again conducted an attack that went too far, putting the full scrutiny of global law enforcement on their operation.

First, it was Colonial Pipeline in 2020, and now it's the attack on UnitedHealth Group's Change Healthcare. The Change Healthcare attack has significantly impacted the US healthcare system after systems used by pharmacies and doctors to file claims with insurance companies were disrupted.

This disruption has led to real-world consequences for US patients who can no longer use discount cards or receive medications under their normal insurance plans, forcing them to temporarily pay full price for critical medications.

The threat actors also claimed to have stolen 6 TB of data from Change Healthcare, containing the healthcare information for millions of US citizens.

After receiving an alleged $22 million ransom payment from Change Healthcare to not leak data and receive the decryptor, an affiliate claimed the BlackCat operators stole their money.

However, instead of being disrupted by law enforcement, the operation has once again shut down, pulling an exit scam.

At this point, it is unclear if the ransomware gang will return under a new name. However, one thing is sure: their reputation has been significantly tarnished, making it doubtful affiliates would want to work with them in the future.

Update [March 6, 10:53]: *Article updated with comment from Europol denying any involvement in a recent disruption of ALPHV ransomware infrastructure.*

Source: https://www.bleepingcomputer.com/news/security/blackcat-ransomware-shuts-down-in-exit-scam-blames-the-feds/