US offers up to $15 million for tips on ALPHV ransomware gang

By Sergiu Gatlan

Published: 2024-02-15 · Archived: 2026-04-05 12:37:31 UTC

The U.S. State Department is offering rewards of up to $10 million for information that could lead to the identification or location of ALPHV/Blackcat ransomware gang leaders.

An additional $5 million bounty is also available for tips on individuals trying to take part in ALPHV ransomware attacks, likely to discourage affiliates and initial access brokers.

The FBI linked this ransomware gang to over 60 breaches worldwide during its first four months of activity between November 2021 and March 2022.


DIE LINKE.
0:00

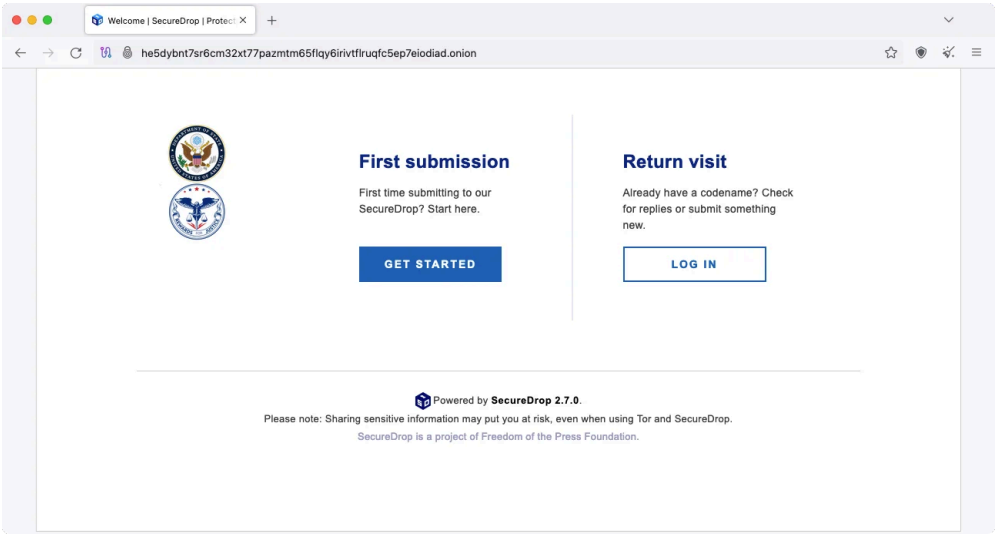
ALPHV has also raked in at least $300 million in ransom payments from more than 1,000 victims until September 2023, according to the FBI.

"The U.S. Department of State is offering a reward of up to $10,000,000 for information leading to the identification or location of any individual(s) who hold a key leadership position in the Transnational Organized Crime group behind the ALPHV/Blackcat ransomware variant," the State Department said.

"In addition, a reward offer of up to $5,000,000 is offered for information leading to the arrest and/or conviction in any country of any individual conspiring to participate in or attempting to participate in ALPHV/Blackcat ransomware activities."

These rewards are provided through the U.S. Transnational Organized Crime Rewards Program (TOCRP), with more than $135 million paid for helpful tips since 1986.

The State Department has set up a dedicated Tor SecureDrop server that can be used to submit tips on ALPHV and other wanted threat actors.



State Department Secure Drop Tor page (BleepingComputer)

Ransomware and pipelines

ALPHV surfaced in November 2021 and is believed to be a rebrand of the DarkSide and BlackMatter ransomware operations.

The operation shut down in May 2021 after extensive investigations by law enforcement led to the seizure of their infrastructure following the Colonial Pipeline attack.

The gang re-emerged under the BlackMatter brand, shut down again in November 2021, and returned as ALPHV/BlackCat in February 2022.

The FBI disrupted ALPHV's operation in December after breaching the group's servers and temporarily taking down its Tor negotiation and leak sites after creating a decryption tool following months of monitoring their activities.

The ransomware gang recently added Canada's Trans-Northern Pipelines to its new leak website, with the company now investigating ALPHV's claims after confirming a November 2023 network breach.

In January, the U.S. government also announced rewards of up to $10 million for information on the leaders of the Hive ransomware gang.

The State Department previously announced bounties of up to $15 million for tips on members and affiliates of the Hive, Clop, Conti [1, 2], REvil (Sodinokibi), and Darkside ransomware operations.

Source: https://www.bleepingcomputer.com/news/security/us-offers-up-to-15-million-for-tips-on-alphv-ransomware-gang/