FBI: ALPHV ransomware raked in $300 million from over 1,000 victims

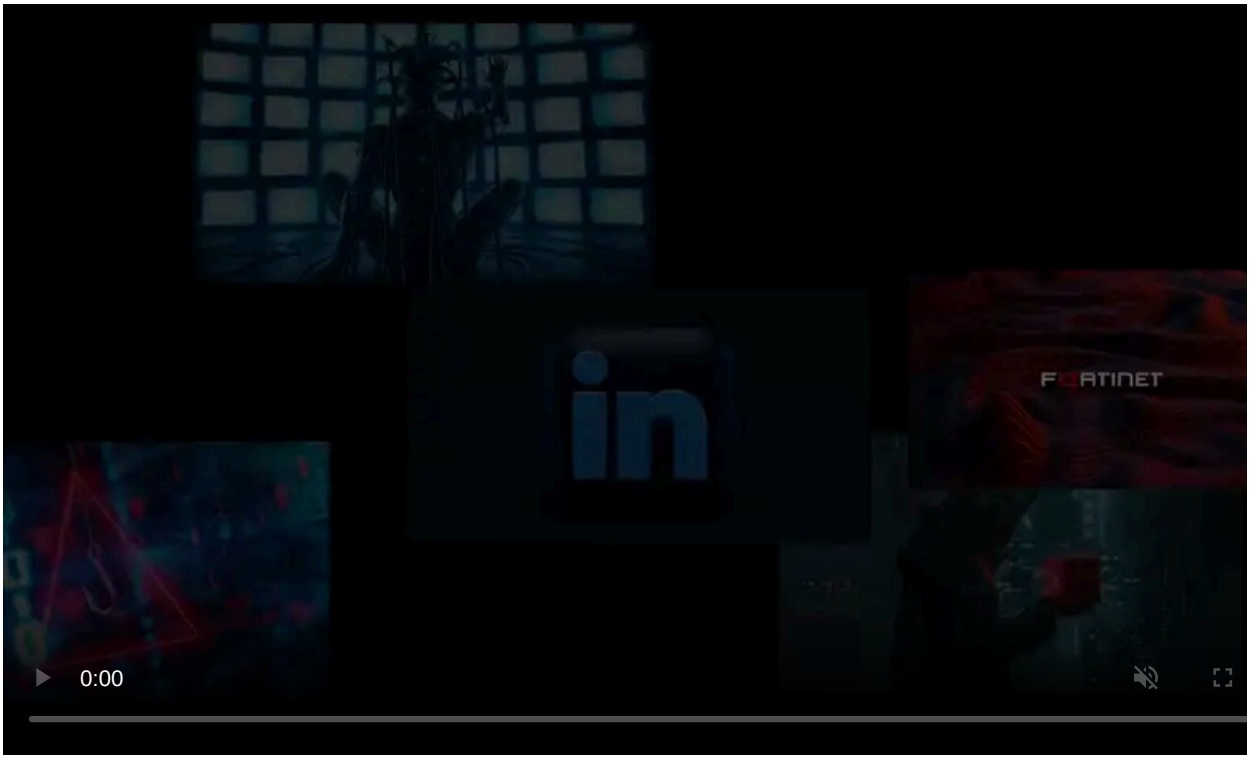
By Sergiu Gatlan

Published: 2023-12-19 · Archived: 2026-04-05 19:39:42 UTC

The ALPHV/BlackCat ransomware gang has made over $300 million in ransom payments from more than 1,000 victims worldwide as of September 2023, according to the Federal Bureau of Investigation (FBI).

"ALPHV Blackcat affiliates have extensive networks and experience with ransomware and data extortion operations," the FBI says.

"According to the FBI, as of September 2023, ALPHV Blackcat affiliates have compromised over 1000 entities—nearly 75 percent of which are in the United States and approximately 250 outside the United States—, demanded over $500 million, and received nearly $300 million in ransom payments."


0:00

In the joint advisory published today in collaboration with CISA, the FBI also shared mitigation measures to help network defenders and critical infrastructure organizations reduce the impact and risks associated with this ransomware group's attacks.

The two agencies also provided ALPHV IOCs (indicators of compromise) and TTPs (tactics, techniques, and procedures) identified by the FBI as recently as December 6.

Network defenders are strongly encouraged to prioritize patching vulnerabilities exploited in the wild and to enforce multifactor authentication (MFA) with strong passwords across all services, especially for webmail, VPN, and accounts linked to critical systems.

Furthermore, they should regularly update and patch software to the latest versions and focus on vulnerability assessments as integral components of standard security protocols.

BlackCat/ALPHV surfaced more than two years ago, in November 2021, and is suspected to be a rebrand of the notorious DarkSide and BlackMatter ransomware operation.

Originally known as DarkSide, this group gained worldwide notoriety following its attack on Colonial Pipeline, leading to extensive investigations by law enforcement agencies.

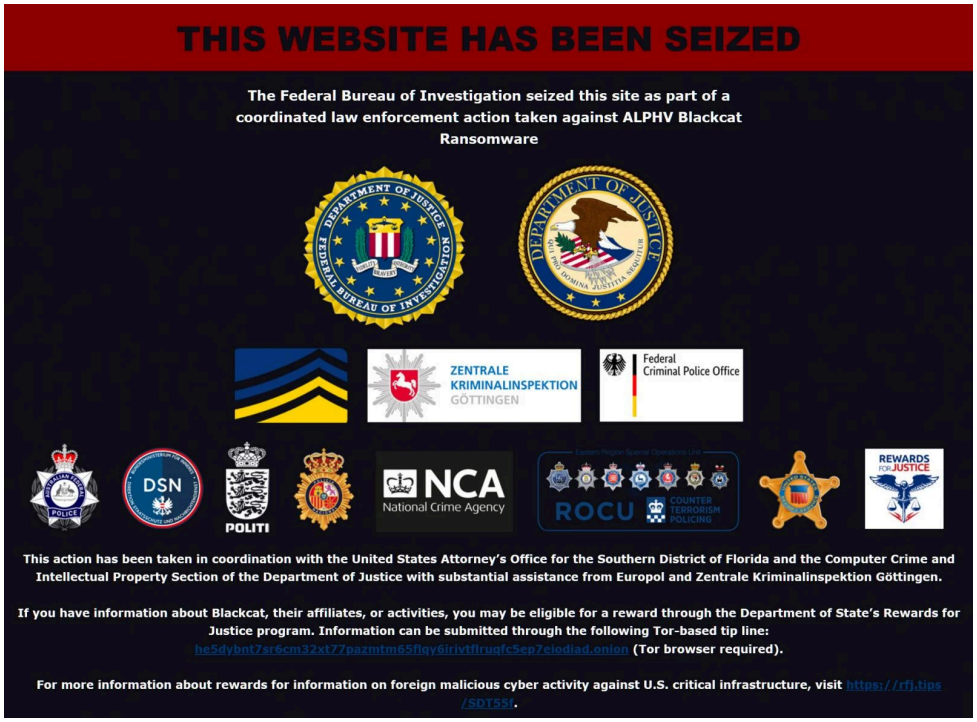
The FBI previously linked this ransomware gang to over 60 breaches impacting organizations worldwide in the first four months of activity, from November 2021 through March 2022.

FBI disrupts Blackcat, develops decryption tool

On December 7, BleepingComputer first reported that ALPHV dark web sites, including the gang's Tor negotiation and data leak websites, suddenly stopped working.

Today, the Department of Justice confirmed our reporting, saying that the FBI breached the ALPHV ransomware operation's servers, successfully monitoring their activities and obtaining decryption keys.

To access ALPHV's backend affiliate panel, the FBI engaged with a confidential human source (CHS) who was provided with login credentials as an affiliate after an interview with the ransomware operators.



ALPHV BlackCat seizure banner (BleepingComputer)

The FBI silently monitored the ALPHV's operations for months while collecting decryption keys, which allowed them to help over 500 victims worldwide recover their files for free, saving around $68 million in ransom demands. However, it's unclear how the private decryption keys were obtained since they wouldn't have been available using an affiliate's backend credentials.

One likely theory, although not yet confirmed, is that the FBI exploited vulnerabilities that allowed dumping the database or gaining further access to the ransomware gang's server.

The FBI also seized the domain for the ransomware operation's data leak site, adding a banner explaining that the seizure was the result of an international law enforcement operation. However, hours later, ALPHV "unseized" their data leak site, claiming that the FBI gained access to a data center hosting the gang's servers. ALPHV also claims in the message posted on their leak site that they've breached at least 3,400 victims.

Since both ALPHV and the FBI currently have the data leak site's private keys, they can take control of the domain from each other.

This situation has been seen as an early holiday gift of sorts by other cybercrime groups, with the LockBit ransomware gang, for instance, asking ALPHV affiliates to switch teams to continue negotiations with victims.

Source: https://www.bleepingcomputer.com/news/security/fbi-alphv-ransomware-raked-in-300-million-from-over-1-000-victims/