BlackCat said they breached US Department of Defense contractor and went offline

Published: 2022-09-30 · Archived: 2026-04-15 02:14:12 UTC

The ransomware gang first said they would leak NJVCs data every 12 hours but later dropped the victim from its list.

Ransomware gang BlackCat, also known as ALPHV, added NJVC, an IT company supporting the federal government and the US Department of Defense, to its victim list.

NJVC provides support for the US government's intelligence and defense organizations. The company boasts a yearly revenue of $290 million.

"[…] the confidential data in our possession will be released in stages every 12 hours. There is a lot of material," said the NJVC description on BlackCat's leak site.

The message appeared on 28 September and was spotted by deep web intelligence firm DarkFeed. Meanwhile, security research group VX-Underground said that BlackCat released a proof of breach and immediately went offline.

Cybernews reached out to NJVC for comment, but we did not receive a reply at the time of publishing this article.

Interestingly enough, BlackCat's leak site on the dark web was accessible on 30 September, but NJVC was no longer posted among the gang's victims. The latest current victim on the leak site was posted on 27 September, a day before the DoD contractor was initially posted.

Experienced 'newcomers'

ALPHV/BlackCat ransomware was first observed in late 2021. Like so many others in the criminal underworld, the group operates a ransomware-as-a-service (RaaS) business, selling criminals malware subscriptions.

ALPHV/BlackCat was noted for the use of the Rust programming language. According to an analysis by the Microsoft 365 Defender Threat Intelligence Team, threat actors that started deploying ALPHV/BlackCat were known to work with other prominent ransomware families such as Conti, LockBit, and REvil.

The FBI believes money launderers for ALPHV/BlackCat cartel are linked to Darkside and Blackmatter ransomware cartels, indicating the group has a well-established network of operatives in the ransomware business.

Lately, ALPHV/BlackCat has been among the most active ransomware gangs. According to the cybersecurity analyst ANOZR WAY, the group was responsible for approximately 12% of all attacks in 2022.

Cybersecurity firm Digital Shadows noted that the group's activity increased by 117% last quarter. Only LockBit and Conti surpassed the group in the total number of victims breached over the second quarter of 2022.

Most recently, ALPHV/BlackCat ransomware was used to attack the University of Pisa. Threat actors demanded that the university administration pay $4.5 million for the release of encrypted data.