ALPHV gang claims ransomware attack on Constellation Software

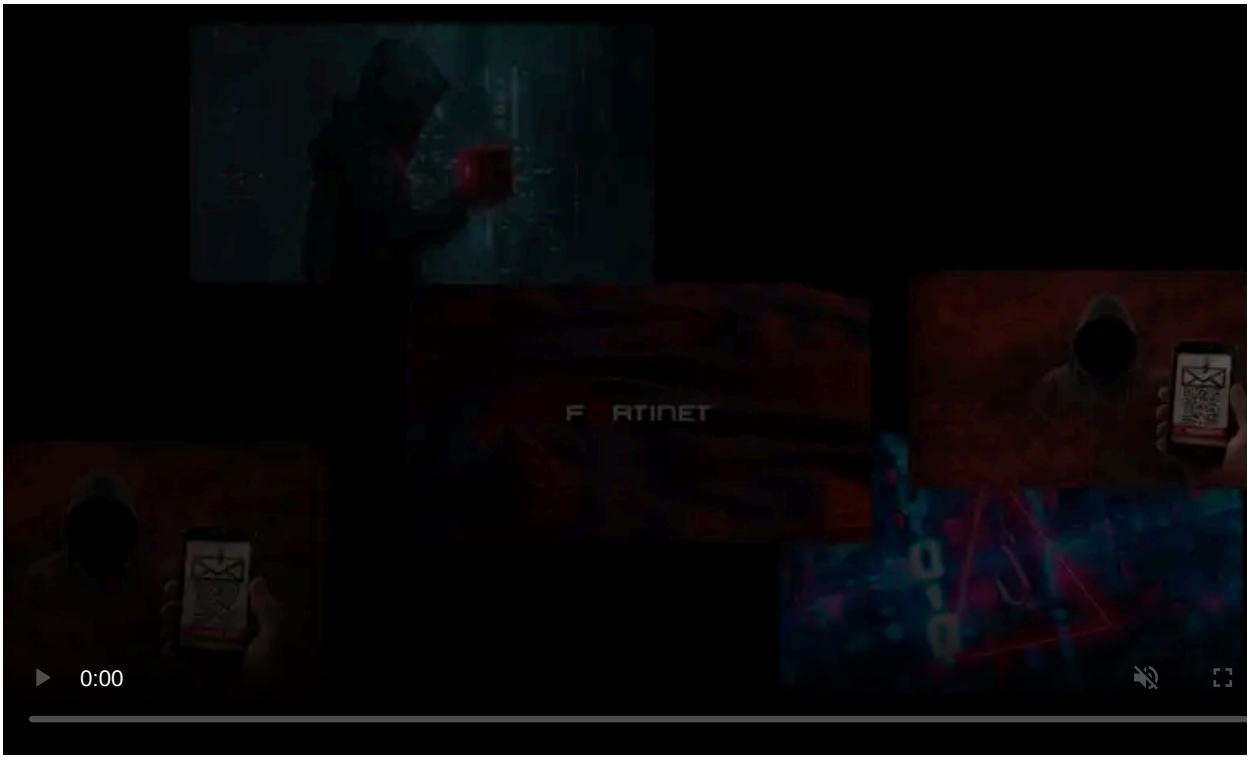
By Sergiu Gatlan

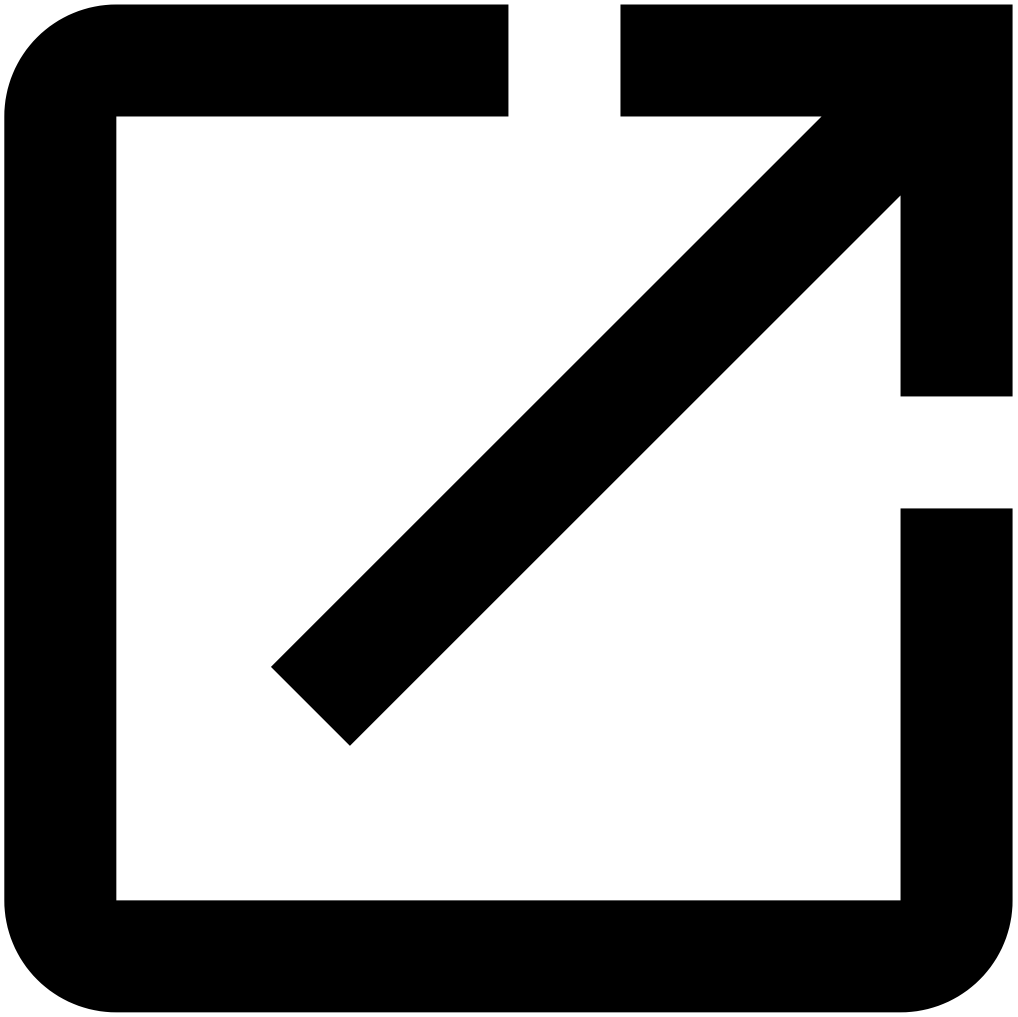
Published: 2023-05-05 · Archived: 2026-04-06 02:06:50 UTC

Canadian diversified software company Constellation Software confirmed on Thursday that some of its systems were breached by threat actors who also stole personal information and business data.

"The Incident was limited to a small number of systems related to internal financial reporting and related data storage by the operating groups and businesses of Constellation," the company said.

"The independent IT systems of Constellation's operating groups and businesses were not impacted by this Incident in any way."


F RTINET
0:00



Constellation added that it had contained the attack and has now restored all of the IT infrastructure systems impacted in the incident.

Business partners and individuals whose information was stolen during the breach are also being contacted with more details regarding the attack.

"A limited amount of personal information of individuals was impacted by the Incident. A limited amount of data of the business partners of Constellation businesses was also impacted," the company added.

Constellation Software acquires, manages, and builds software businesses through six operating groups: Volaris, Harris, Jonas, Vela Software, Perseus Group, and Topicus.

The Canadian company has over 25,000 employees across North America, Europe, Australia, South America, and Africa, generating consolidated revenues exceeding $4 billion.

Constellation also provides services to 125,000 customers in over 100 countries and has acquired more than 500 software companies since 1995.

Attack claimed by the ALPHV ransomware gang

While Constellation is yet to provide information on who was behind the attack or how the threat actors gained access to its network, the ALPHV ransomware gang (aka BlackCat) added a new entry to its data leak site, saying that they breached the company's network and stole more than 1 TB worth of files.

The ransomware gang also threatens to leak the stolen data if the company ignores the ransom demand and refuses to negotiate.

"We have been on your network for a long time and have had time to analyze your business. We have stolen more than 1 TB of your confidential data. If you ignore or refuse the deal, we will be forced to release all of your data to the public," the gang said.

As proof that they had access and exfiltrated files from Constellation's network, ALPHV has already leaked some documents containing business information online.

Constellation Software entry on ALPHV's data leak blog (BleepingComputer)

This ransomware operation was launched in November 2021 and is believed to be a rebrand of the DarkSide/BlackMatter gang.

It first gained notoriety as DarkSide after attacking the Colonial Pipeline and immediately landing in the crosshairs of international law enforcement.

Even though they rebranded as BlackMatter one month later, in July 2021, they were forced to shut down again in November after the operation's servers were seized and Emsisoft created a decryptor by exploiting a weakness in the ransomware.

Currently, the ALPHV gang is considered one of the significant ransomware threats targeting enterprises worldwide.

Last April, the Federal Bureau of Investigation (FBI) warned that ALPHV has "extensive networks and experience with ransomware operations" since they successfully breached over 60 entities worldwide from November 2021 to March 2022.

Source: https://www.bleepingcomputer.com/news/security/alphv-gang-claims-ransomware-attack-on-constellation-software/