Trans-Northern Pipelines investigating ALPHV ransomware attack claims

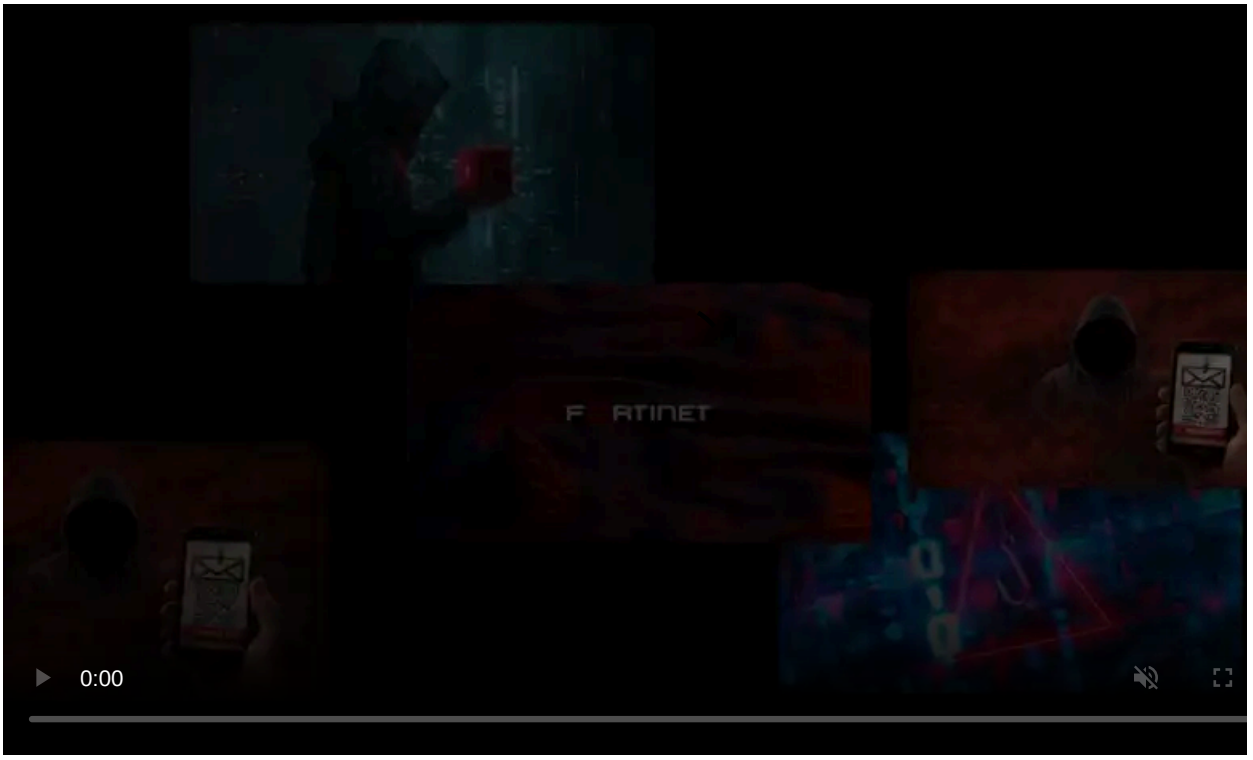
By Sergiu Gatlan

Published: 2024-02-14 · Archived: 2026-04-05 22:45:32 UTC

Trans-Northern Pipelines (TNPI) has confirmed its internal network was breached in November 2023 and that it's now investigating claims of data theft made by the ALPHV/BlackCat ransomware gang.

TNPI operates 850 kilometers (528 miles) of pipeline in Ontario-Quebec and 320 kilometers (198 miles) in Alberta, transporting 221,300 barrels (35.200m^3) of refined petroleum products daily.

Both pipeline systems are underground and transport gasoline, diesel fuel, aviation fuel, and heating fuel from refineries to distribution terminals.


F RTINET
0:00

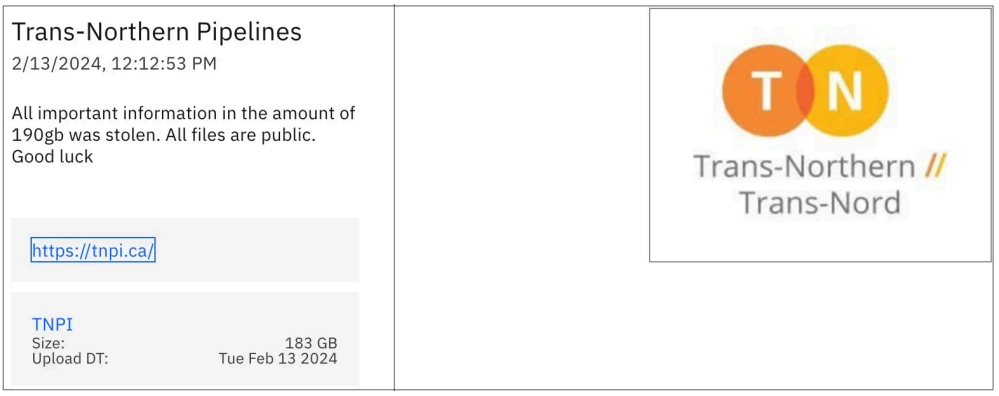
"Trans-Northern Pipelines Inc. experienced a cybersecurity incident in November 2023 impacting a limited number of internal computer systems," TNPI Communications Team Lead Lisa Dornan told BleepingComputer.

"We have worked with third-party, cybersecurity experts and the incident was quickly contained. We continue to safely operate our pipeline systems.

"We are aware of posts on the dark web claiming to contain company information, and we are investigating those claims."

While ALPHV's claims were not directly mentioned by Dornan when asked by BleepingComputer for confirmation, the ransomware gang says its operators stole 183GB of documents from the company's network.

The allegedly stolen files have now been published on ALPHV's data leak site, and the ransomware group has also added contact information for several TNPI employees to the same leak page.



TNPI entry on ALPHV's leak site (BleepingComputer)

ALPHV emerged over two years ago, in November 2021, and is believed to be a rebrand of the DarkSide and BlackMatter ransomware operations.

Initially tracked as DarkSide, the operation gained notoriety after their Colonial Pipeline attack, which prompted extensive investigations by law enforcement agencies worldwide and led to the seizure of their infrastructure and the operation's shutdown.

Months later, the ransomware group returned under the BlackMatter name, which again shut down in November 2021 and resurfaced as ALPHV/BlackCat in February 2022.

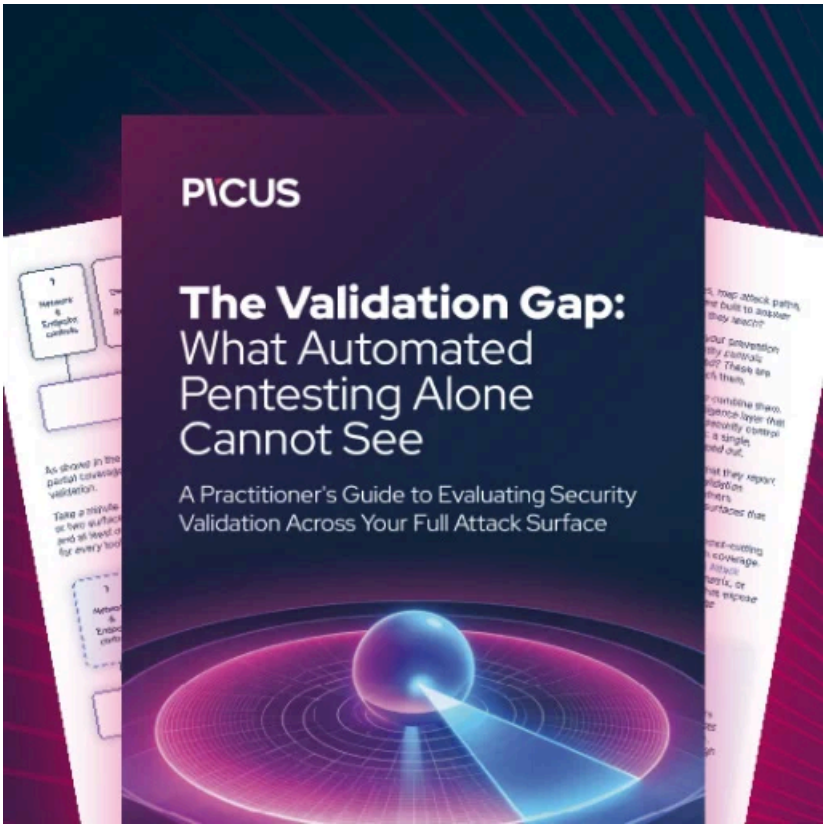
The FBI linked this ransomware gang to more than 60 breaches against organizations worldwide during its first four months of activity, between November 2021 through March 2022.

ALPHV amassed over $300 million in ransom payments from over 1,000 victims worldwide until September 2023, according to the Federal Bureau of Investigation (FBI).

"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," the FBI said in December.

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

The ransomware gang has since "unseized" their data leak site using the private keys they still owned and launched a new Tor URL the FBI can't take down.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/trans-northern-pipelines-investigating-alphv-ransomware-attack-claims/