ALPHV ransomware claims loanDepot, Prudential Financial breaches

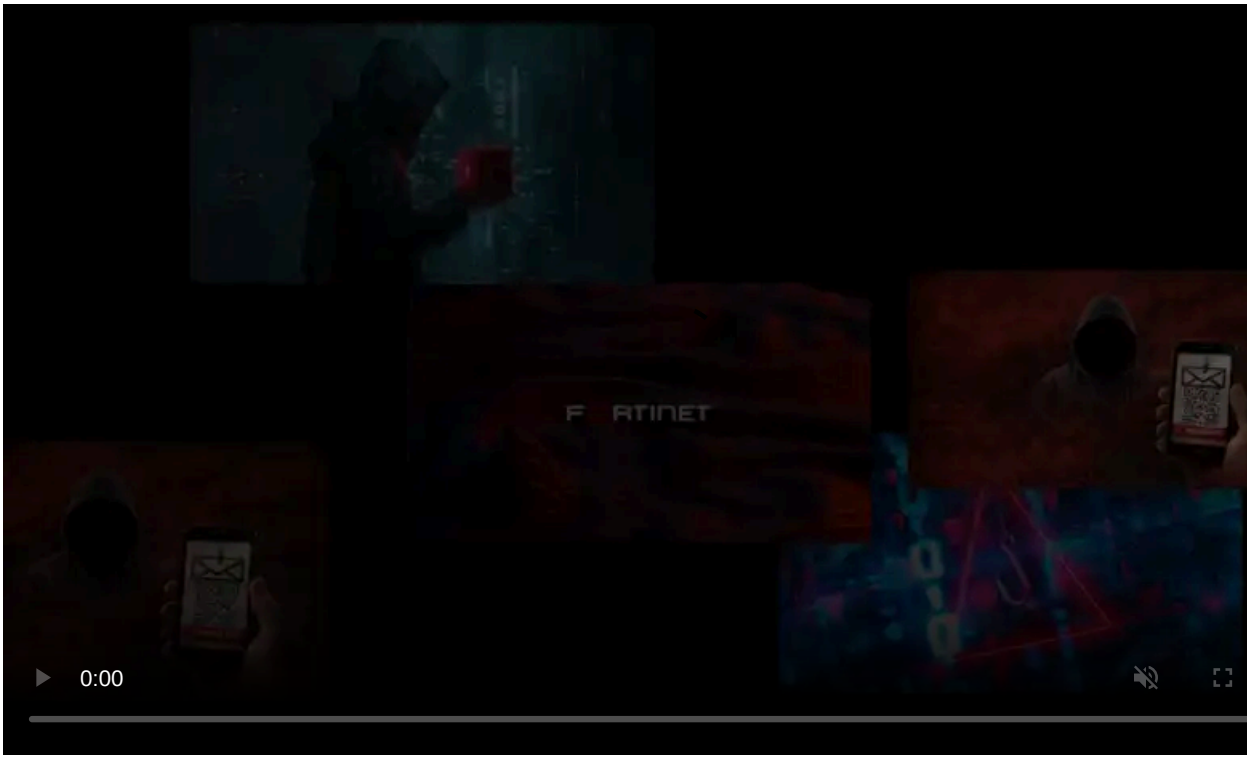
By Sergiu Gatlan

Published: 2024-02-16 · Archived: 2026-04-06 00:40:39 UTC

The ALPHV/Blackcat ransomware gang has claimed responsibility for the recent network breaches of Fortune 500 company Prudential Financial and mortgage lender loanDepot.

The two companies were added to ALPHV's dark web leak site today, with the threat actors still having to publish proof of their claims. ALPHV plans to sell the stolen data from loanDepot's network and release Prudential's data for free after failed negotiations.

loanDepot revealed on January 22 that at least 16.6 million people had their personal information stolen in the ransomware attack they confirmed on January 8, two days after disclosing it as a "cyber incident" on January 6.


F RTINET
0:00

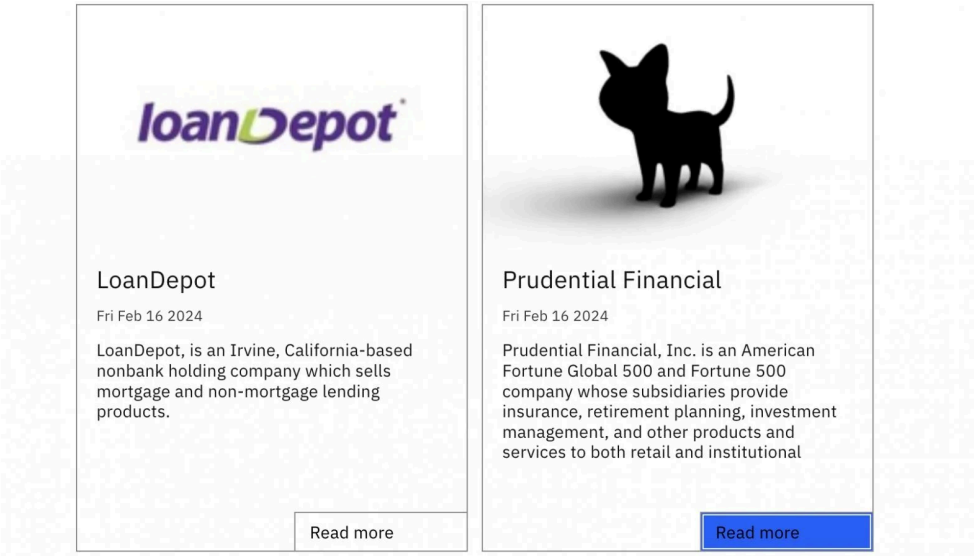
The company said it would notify those impacted by the data breach and provide them with free credit monitoring and identity protection services.

loanDepot is one of the largest U.S. nonbank retail mortgage lenders, with roughly 6,000 employees and over $140 billion in serviced loans.

On Tuesday, Prudential Financial also revealed that a suspected cybercrime group breached its network on February 4 and stole employee and contractor data.

Prudential said an ongoing investigation assesses the incident's full scope and impact but has yet to find evidence that the attackers also exfiltrated customer or client data.

This leading global financial services Fortune 500 company is the second-largest life insurance company in the U.S., with reported revenues of more than $50 billion in 2023, and it employs 40,000 people worldwide.



loanDepot and Prudential entries on ALPHV's leak site (BleepingComputer)

On Thursday, the U.S. State Department announced rewards of up to $10 million for tips that could lead to the identification or location of ALPHV gang leaders.

An additional $5 million reward is offered for information on individuals linked to or attempting to participate in ALPHV ransomware attacks.

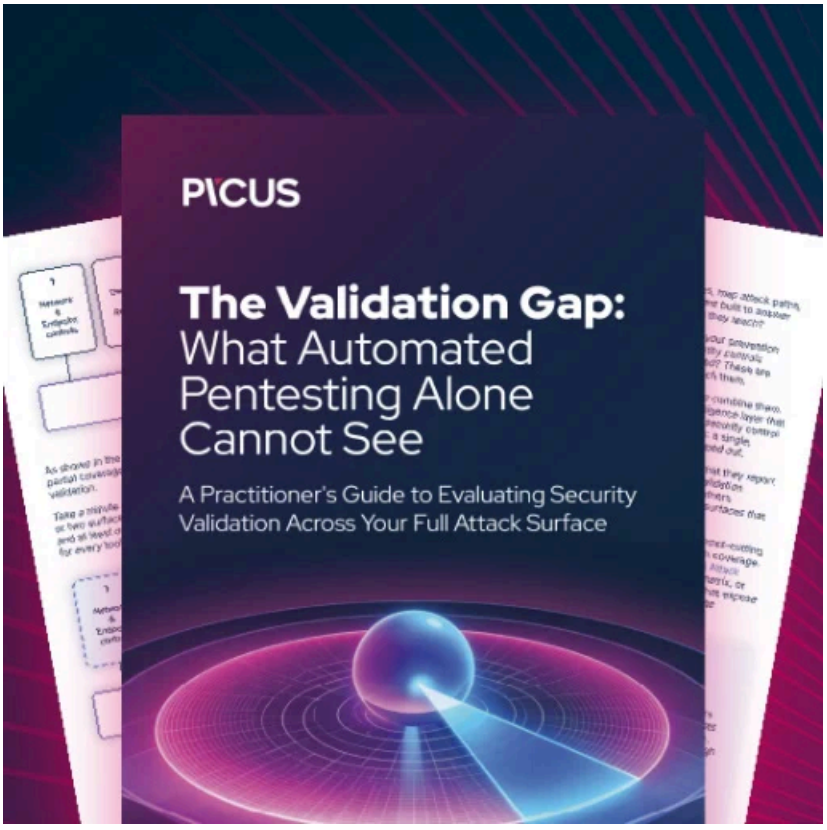
The FBI linked this gang to over 60 breaches worldwide during its first four months of activity between November 2021 and March 2022. The law enforcement agency also estimates that ALPHV raked in at least $300 million in ransom payments from over 1,000 victims until September 2023.

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

The group gained worldwide notoriety after the Colonial Pipeline attack, which led to extensive investigations by law enforcement agencies worldwide and the operation going through two rebrands.

The FBI disrupted the gang's operation in December and temporarily took down its Tor negotiation and leak sites after breaching its servers months earlier and creating a decryption tool.

ALPHV has since "unseized" their data leak site with the help of private keys they still owned and has now launched a new Tor leak site the FBI has yet to 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/alphv-ransomware-claims-loandepot-prudential-financial-breaches/