BlackCat ransomware claims breach of healthcare giant Henry Schein

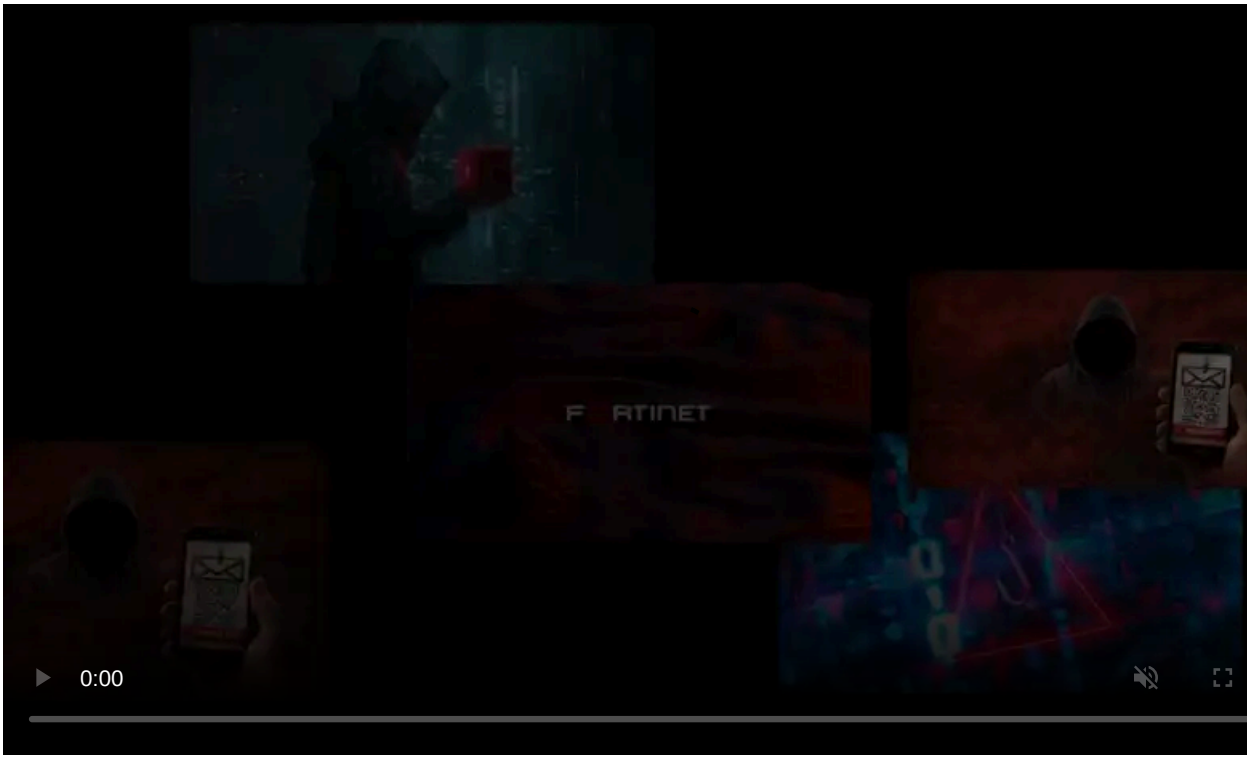
By Sergiu Gatlan

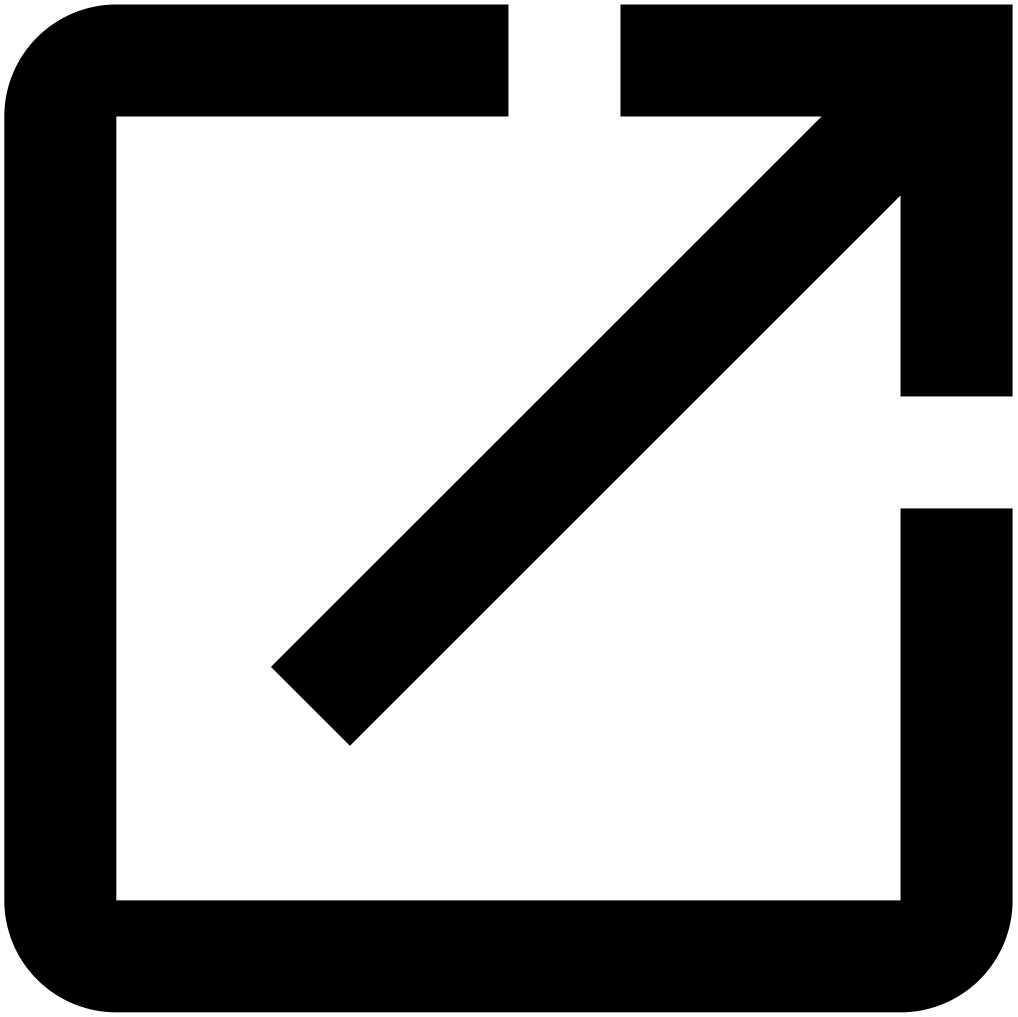
Published: 2023-11-02 · Archived: 2026-04-05 20:29:49 UTC

The BlackCat (ALPHV) ransomware gang claims it breached the network of healthcare giant Henry Schein and stole dozens of terabytes of data, including payroll data and shareholder information.

Henry Schein is a healthcare solutions provider and a Fortune 500 company with operations and affiliates in 32 countries and revenue of over $12 billion in 2022.

The company disclosed on October 15 that it was forced to take some systems offline to contain a cyberattack that impacted its manufacturing and distribution businesses one day before.


F RTINET
0:00



"Henry Schein promptly took precautionary action, including taking certain systems offline and other steps intended to contain the incident, which has led to temporary disruption of some of Henry Schein's business operations. The Company is working to resolve the situation as soon as possible," it said.

While some of its business operations were disrupted, the company says its Henry Schein One practice management software has not been impacted.

Henry Schein notified relevant law enforcement authorities of the incident and has since hired external cybersecurity and forensics experts to investigate a potential data breach stemming from the attack.

In a letter published one week after disclosing the cyberattack, the healthcare services provider urged customers to place orders through their Henry Schein representative or using dedicated telesales phone numbers.

A Henry Schein spokesperson was not immediately available for comment when contacted by BleepingComputer earlier today.

BlackCat claims Henry Schein breach

Almost two weeks later, the BlackCat/ALPHV ransomware group has added Henry Schein to its dark web leak site, claiming that they breached the company's network and stole 35 TB of sensitive files.

The gang claims they encrypted the company's devices again just as Henry Schein almost finished restoring all its systems because ongoing negotiations failed.

"Despite ongoing discussions with Henry's team, we have not received any indication of their willingness to prioritize the security of their clients, partners, and employees, let alone protect their own network," the threat actors said.

"As of midnight today, a portion of their internal payroll data and shareholder folders will be published on our collections blog. We will continue to release more data daily."

Henry Schein's entry on BlackCat's data leak site has since been deleted, hinting at the company restarting negotiations or paying the ransom.

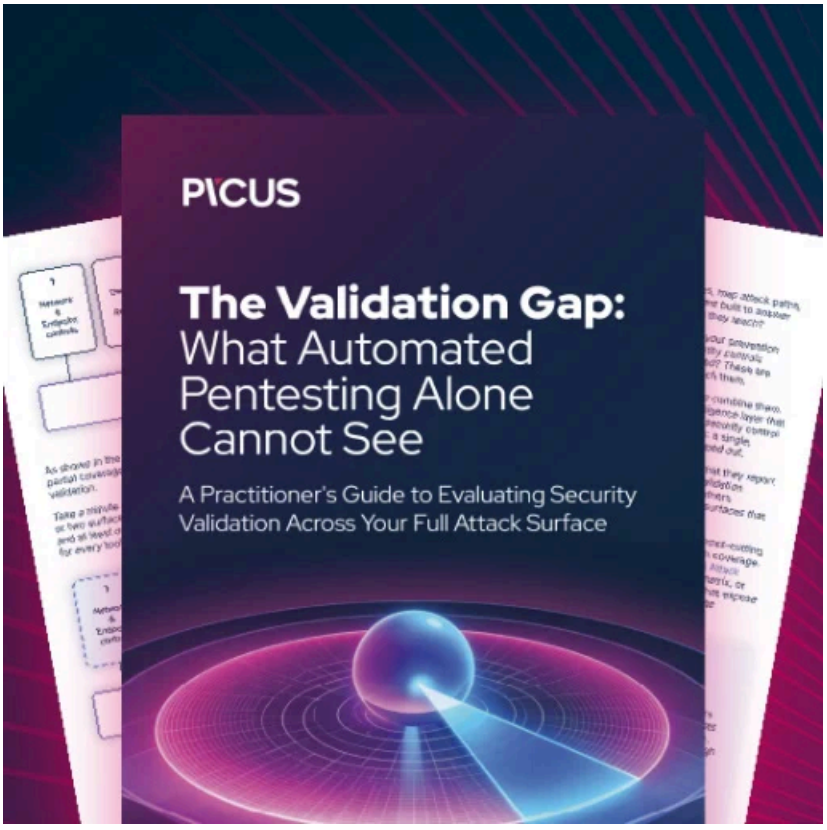
The BlackCat ransomware operation surfaced in November 2021 and is suspected to be a rebrand of the notorious DarkSide/BlackMatter group.

Initially known as DarkSide, the cybercrime gang drew global attention after infiltrating Colonial Pipeline, prompting law enforcement investigations worldwide.

More recently, a BlackCat affiliate tracked as Scattered Spider claimed responsibility for the MGM Resorts breach, allegedly encrypting over 100 ESXi hypervisors after MGM Resorts refused ransom negotiations and shut down its internal infrastructure.

In April 2022, the FBI linked the group to successful attacks on more than 60 organizations worldwide between November 2021 and March 2022.

H/T Dominic Alvieri



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/blackcat-ransomware-claims-breach-of-healthcare-giant-henry-schein/