ALPHV ransomware gang claims attack on Florida circuit court

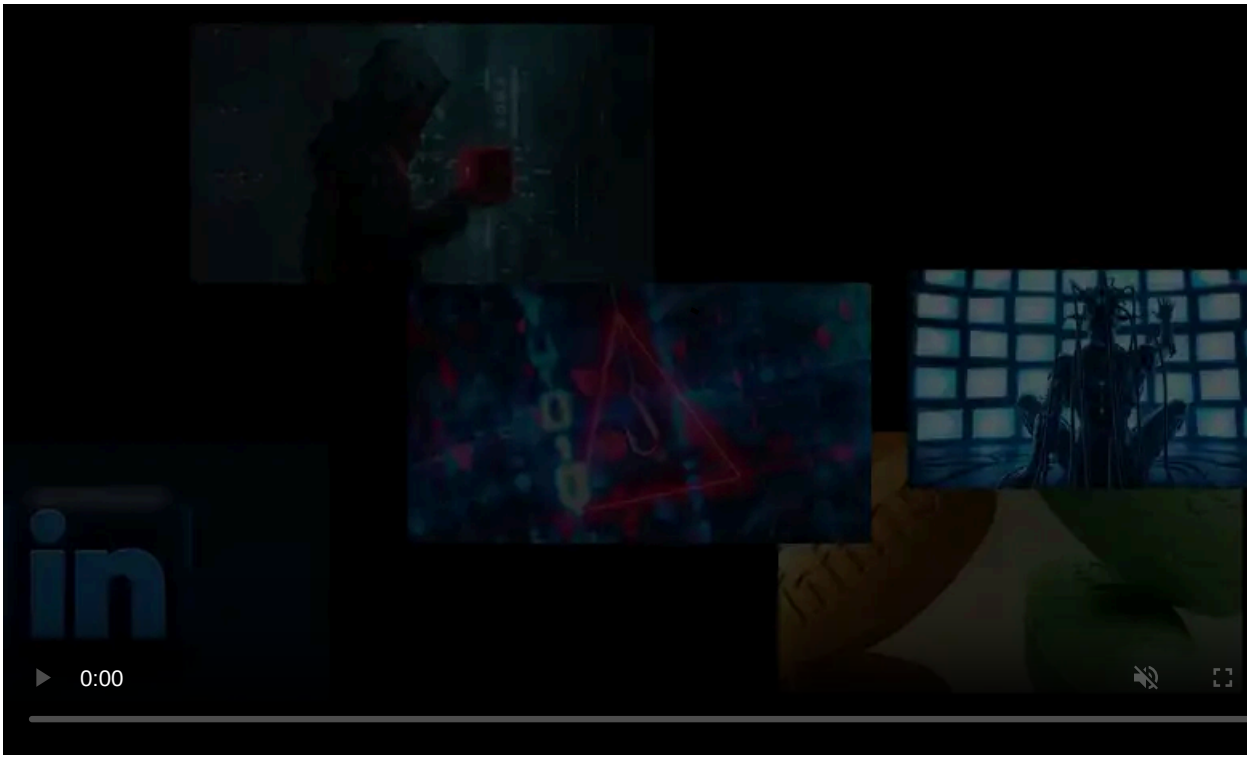
By Sergiu Gatlan

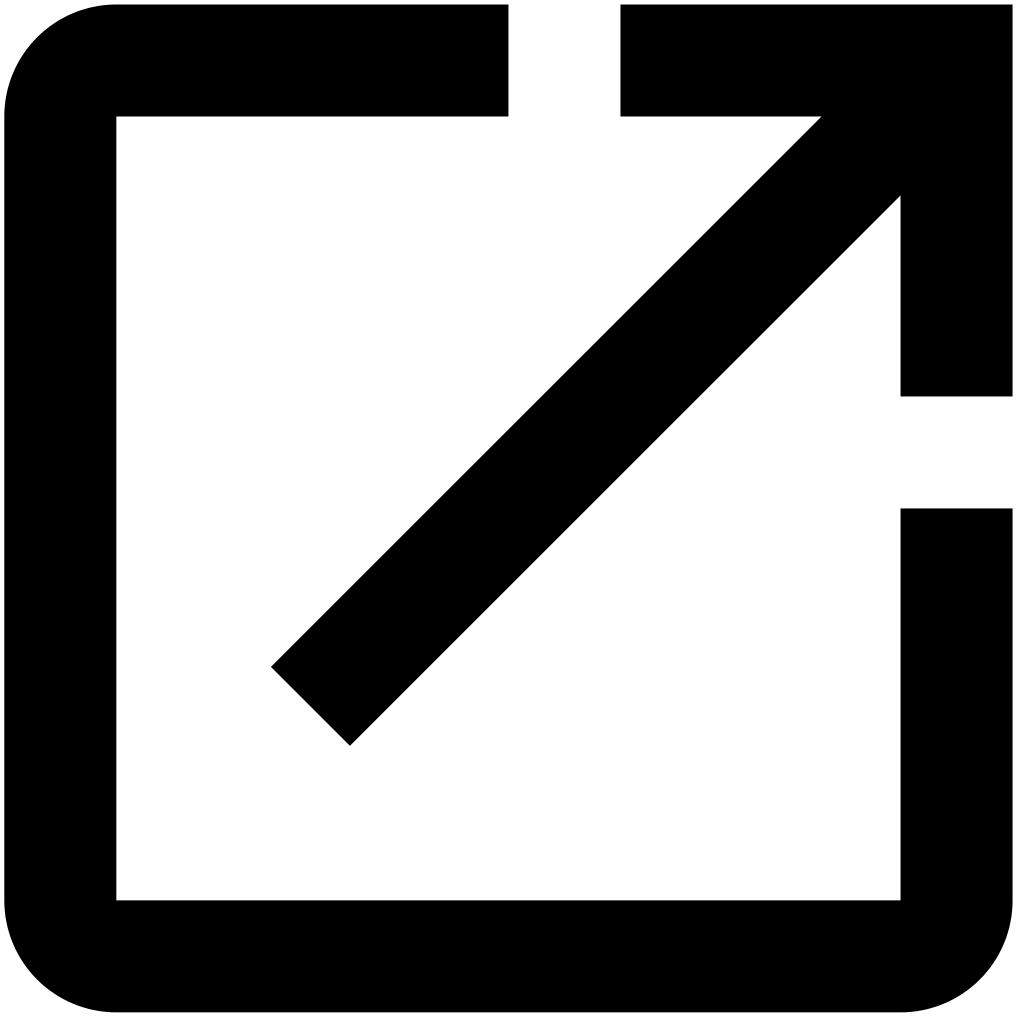
Published: 2023-10-09 · Archived: 2026-04-05 16:10:45 UTC

The ALPHV (BlackCat) ransomware gang has claimed an attack that affected state courts across Northwest Florida (part of the First Judicial Circuit) last week.

Allegedly, the threat actors have acquired personal details like Social Security numbers and CVs of employees, including judges.

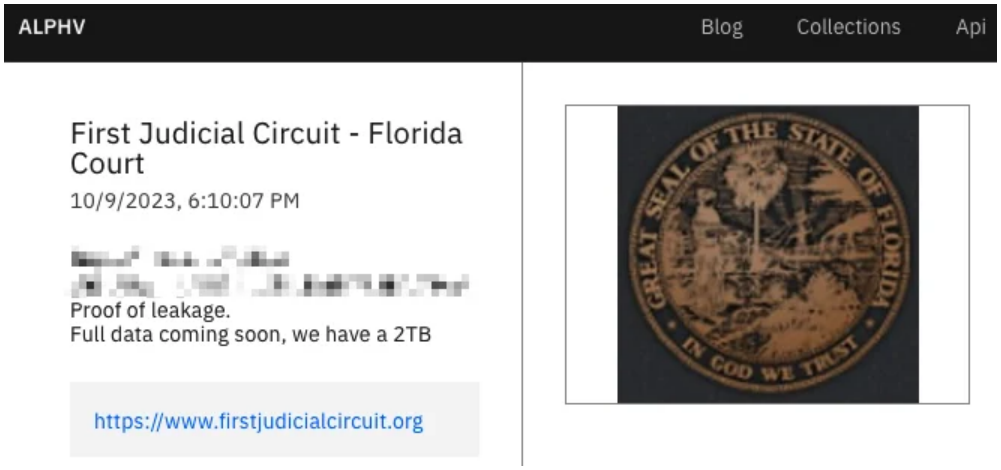
Additionally, ALPHV claims to possess a comprehensive network map of the court's systems, complete with local and remote service credentials.


0:00



Ransomware gangs commonly threaten to leak stolen data online to coerce victims into negotiation or reopening discussions.

The presence of Florida's First Judicial Circuit's data leak page on ALPHV's website suggests that the court has either not engaged in negotiations with the ransomware operation or has firmly declined to meet the gang's demands.



Florida First Judicial Circuit ALLPHV data leak page (BleepingComputer)

Breached last week

The Florida circuit court disclosed last week that it was investigating a cyberattack that disrupted its operations on Monday morning, October 2nd.

"This event will significantly affect court operations across the Circuit, impacting courts in Escambia, Okaloosa, Santa Rosa, and Walton counties, for an extended period," a statement published on the court's website says.

"The Circuit is prioritizing essential court proceedings but will cancel and reschedule other proceedings and pause related operations for several days, beginning Monday, October 2, 2023."

Amid the ongoing investigation into the attack, judges in the four counties have been communicating with litigants and attorneys regarding their weekly scheduled hearings.

Additionally, the court authorities confirmed that all facilities continue operating without disruptions. The court has not yet verified the ransomware attack claims made by the ALPHV gang.

The ALPHV ransomware operation

The BlackCat/ALPHV ransomware operation surfaced in November 2021 and is believed to be a rebranding of DarkSide/BlackMatter.

Initially known as DarkSide, the group gained international attention following the breach of Colonial Pipeline, leading to scrutiny from law enforcement agencies globally.

After rebranding again as BlackMatter in July 2021, their operations abruptly ceased in November 2021 when authorities seized their servers, and security firm Emsisoft created a decryptor exploiting a ransomware vulnerability.

This ransomware operation is known for consistently targeting global enterprises and continuously adapting and refining their tactics.

In a recent incident, an affiliate tracked as Scattered Spider claimed responsibility for the attack on MGM Resorts, claiming to have encrypted over 100 ESXi hypervisors after the company shut down internal infrastructure and declined to negotiate a ransom.

As BleepingComputer reported last week, ALPHV's ransomware attack on MGM Resorts led to losses of approximately $100 million, as well as the theft of its customers' personal information.

The FBI issued a warning in April, highlighting the group's involvement in successful breaches of over 60 entities worldwide between November 2021 and March 2022.

H/T Dominic Alvieri

Source: https://www.bleepingcomputer.com/news/security/alphv-ransomware-gang-claims-attack-on-florida-circuit-court/