Legal services platform used by SEC, Pentagon investigating ransomware attack claims

By Jonathan Greig

Published: 2023-06-02 · Archived: 2026-04-05 14:05:26 UTC

A legal document platform used by several arms of the U.S. government is investigating claims by a ransomware group that it has been attacked.

Casepoint, based outside of Washington, D.C., provides organizations with a platform to post legal documents for litigation, investigations and compliance.

In April the company signed a five-year deal with the United States Courts Defender Services Office and provides services to the Securities and Exchange Commission, the U.S. Department of Defense, the U.S. Department of Veterans Affairs, the USDA, Marriott and more.

But this week, the BlackCat/AlphV ransomware group added Casepoint to its list of victims, sharing several sensitive documents allegedly related to the FBI and claiming to have access to the company's network.

James Lasson, Casepoint's vice president of marketing, initially told Recorded Future News that there was "no validation that a breach has occurred."

"We have not heard anything from the cyber group for a ransom. We have not seen any unusual activity on our networks that would suggest out of the ordinary data movement off our systems. We are working with the FBI to determine the appropriate next steps," he said.

"SEC, DOD and other government clients are on a different network than our commercial clients."

In a follow-up statement, a spokesperson for the company said it activated its incident response protocols on Tuesday and hired a forensic firm to help investigate the allegations. The firm is serving "as an extra set of eyes on the remediation work we've already performed to date," the company said.

But they reiterated that the company is fully operational and has not experienced any disruption to its services. Its clients have been able to continue using the platform as usual, they added.

The forensic firm is in the process of running scans and deploying advanced endpoint detection monitoring tools, looking for signs of suspicious activity.

"We are early on in our investigation and are committed to keeping our clients informed as we learn more," the spokesperson said.

"We're on top of it, and we know transparency and proactivity is key to a good response to these types of matters. We appreciate the trust our customers and employees put in Casepoint and will do everything we can to continue earning it."

The company did not respond to follow-up questions asking whether the documents leaked by the ransomware gang were legitimate and came from the platform.

BlackCat claimed to have 2 terabytes of data from Casepoint and provided a wide variety of samples. The gang has in the past claimed to attack major companies like Ring that were later denied by victims.

Many experts said the hackers associated with the ransomware gang were also the people behind the Darkside ransomware group – which was responsible for the cyberattack on Colonial Pipeline.

Jonathan Greig

is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.