

# Officials: Virginia IT agency hit with ransomware attack

December 13 2021, by Sarah Rankin and Alan Suderman

---



This Sunday, Jan. 19, 2020, file photo shows the Virginia State Capitol in Richmond, Va. A Virginia legislative branch agency has been hit by a ransomware attack, Gov. Ralph Northam's office said Monday, Dec. 13, 2021. The timing of the attack is particularly problematic, as lawmakers and staff are deep into preparations for a legislative session set to start in January. Credit: AP Photo/Steve Helber

The information technology agency that serves Virginia's legislature has

been hit by a ransomware attack that has substantially affected its operations, state officials said Monday.

Gov. Ralph Northam's spokeswoman, Alena Yarmosky, confirmed the attack on Virginia's Division of Legislative Automated Systems. In a brief statement provided to The Associated Press, Yarmosky said the governor had been briefed on the matter and directed executive branch agencies to offer help in "assessing and responding to this ongoing situation."

The Division of Legislative Automated Systems, or DLAS, is the General Assembly's IT agency. The timing of the attack is particularly problematic, as lawmakers and staff are deep into preparations for a legislative session set to start in January.

The attack marks the latest in [a ransomware scourge](#) that has [exploded](#) over the past year, with attacks against governments, critical infrastructure and major corporations.

Cybersecurity researchers who track ransomware say there's no previous record of a state legislature suffering an attack.

"It continues to show that no organization is safe from these ransomware attacks. Anybody anywhere can be hit," said Allan Liska, an intelligence analyst at the cybersecurity firm Recorded Future.

A top agency official told Virginia legislative leaders in an email obtained by The Associated Press that hackers using "extremely sophisticated malware" had accessed the system late Friday.

A ransom note with no specific amount or date was sent, according to the email sent Monday afternoon by Dave Burhop.

The agency was working with authorities to determine "the scope of the issue and plan for possible remediation," Burhop wrote. All of the agency's internal servers, including those for bill drafting, the budget system and the General Assembly voicemail system, were affected, the email said.

"Anything to do with bill drafting or bill referrals—all of that has been impacted," Senate Clerk Susan Clarke Schaar said.

Burhop's email said his agency was collaborating with law enforcement agencies including the FBI. An FBI spokesman declined comment.

The email also said cybersecurity firm Mandiant had been retained since a "breach" over the summer involving the use of an employee's credentials and was assisting in the investigation. A company spokesperson declined comment.

"After upcoming meetings, we will provide additional information, including a course of action to this leadership group but please understand this likely will not be resolved quickly," wrote Burhop, who couldn't immediately be reached for further comment.

Brett Callow, a threat analyst at the firm Emsisoft, said Virginia is the 74th state or local government hit by ransomware attacks this year, though the first legislature he's ever seen attacked.

"Honestly, I'm surprised it hasn't happened before," Callow said.

Liska said it's not uncommon for ransomware gangs to try to time their attacks to inflict maximum pain on the targets, like some hackers have done to school districts just at the start of a school year.

"They are smart enough to do that," he said.

The website for the Division of Capitol Police was also down as a result of the attack. But a spokesperson said the agency was operational, with its critical communications functions unaffected.

Although DLAS does not fall within the purview of the Virginia Information Technologies Agency, which oversees IT for the state's executive branch, a VITA spokesperson said the agency was also helping with the response effort.

There were so far no indications that the attack had affected any executive branch agencies, the spokesperson, Stephanie Benson, said.

© 2021 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed without permission.

Citation: Officials: Virginia IT agency hit with ransomware attack (2021, December 13)  
retrieved 19 April 2024 from  
<https://techxplore.com/news/2021-12-virginia-state-agency-ransomware.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.