Cybersecurity officials warn state and local agencies (again) to fend off ransomware

Enlarge / Georgia State Police and Capitol Police had their laptops taken offline by ransomware in the latest of many attacks on state and local government agencies.

reader comments

34 with 23 posters participating

Share this story

Yesterday, the Georgia Department of Public Safety revealed that laptop computers in state police and Capitol police vehicles—as well as laptops used by Georgia's Motor Carrier Compliance Division (the officers who operate trucking scales and safety spot checks)—had been taken offline by ransomware. The attack comes a week after Louisiana Governor John Bel Edwards declared a statewide emergency after "a malware attack on a few North Louisiana school systems," bringing state resources to assist in the response. And also last week, the city power company in Johannesburg, South Africa, was hit by ransomware, taking down payment systems and causing power outages.

These are just the latest episodes in a long line of state and local government organizations that have fallen to ransomware attacks. As Louisiana was declaring a state of emergency, the Board of Estimates of the City of Baltimore was approving $10

million in spending to recover from the city's nearly month-long IT outage caused by the RobbinHood ransomware. So today, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), the Multi-State Information Sharing and Analysis Center (MS-ISAC), the National Governors Association (NGA), and the National Association of State Chief Information Officers (NASCIO) issued a warning urging organizations to take immediate steps to protect themselves against ransomware attacks. The hope is that state and local agencies will heed the warning and blunt the damage being done by recent ransomware variants.

The three steps urged by CISA, MS-ISAC, NGA, and NASCIO are fairly basic security hygiene: run daily backups, train staff on "cybersecurity awareness," and "revisit and refine cyber incident response plans." Unfortunately, these three steps may be beyond the capabilities of the organizations most likely to be hit by ransomware—school districts, government agencies, and small and mid-sized businesses that have IT budgets that place them below the information security poverty line.

Monroe City Schools in Louisiana apparently had backups in place and managed to respond quickly to what Superintendent Brent Vidrine confirmed was a targeted ransomware attack. The attack shared techniques used in the Ryuk ransomware strikes on a pair of Florida local governments and Georgia's Judicial Council and Administrative Office of the Courts last month.

"They were given some email addresses, but we did not contact anybody," Vidrine said during a July 16 school board meeting. "We had our systems protected."

The school system's IT department restored servers from a previous backup and was sweeping all computer systems for remaining malware before bringing them back onto the network. An investigation is ongoing.

But many school systems remain at risk. As Ars has previously

reported, many districts are particularly vulnerable to ransomware attacks; based on security scan data, many school districts in the United States still have systems running vulnerable versions of the Windows SMB file sharing protocol directly exposed to the Internet. A review of recent data found more than 600 servers associated with school districts still running SMB version 1 on systems exposed to the Internet—more than two years after Microsoft issued patches and warnings about the vulnerability of those systems and a National Security Agency exploit of that vulnerability was leaked by Shadow Brokers.

In a press release today, a spokesperson for Louisiana's Sabine Parish School Board said that the attack on the school system's networks is "still under investigation," and that state agencies—including the Louisiana Office of Technology Services, National Guard and Air National Guard "are aiding in these efforts." The spokesperson said that there was no evidence that student or staff personal data was stolen in the attack. School is scheduled to open on August 12 in Sabine Parish; there's no word on whether the ransomware attack will affect that scheduled start date.

https://arstechnica.com/?p=1543587