Cyberattack disrupts unemployment benefits in some states

June 30 2022, By JONATHAN MATTISE and ALAN SUDERMAN

Credit: CC0 Public Domain

A cyberattack on a software company has disrupted unemployment benefits and job seeking assistance for thousands of people in several states.

In Tennessee, the website for unemployment benefits remained down Thursday morning after the vendor, Geographic Solutions Inc., told the state Sunday that service would be interrupted. Some 12,000 Tennesseans rely on the unemployment program, and for now, they're not getting their payments.

The company said that it expects Tennessee's system to be back online before July 4.

"With a recession looming, it is unacceptable that Tennesseans cannot receive the unemployment benefits they deserve," said state Republican Sen. Paul Bailey, commerce and labor committee chairman.

In a statement dated Wednesday evening, Geographic Solutions' president said initial investigation findings indicate that no personal data was accessed and no data was removed from its network operations center.

The president, Paul Toomey, said his company identified "anomalous activity" on its network and immediately took the Tennessee system offline to halt the activity.

"With the help of third-party specialists, we are conducting a full investigation to determine the cause and scope of the incident," Toomey said. "That investigation is still ongoing, and we are taking steps to help prevent this from happening again."

Unemployment websites in several other states were affected too. In Louisiana, people seeking to file unemployment online are directed instead to use a call center instead. The website to file claims in Nebraska was taken offline and the state said it did not have an exact timeline for when it would be back up.

"Individuals cannot file for unemployment until the system is back online," Nebraska Department of Labor spokeswoman Grace Johnson said in an email.

It's still unclear if it was a ransomware attack or some other type of cyber incident that affected Geographic Solutions. Nor it is clear how many states are affected.

Geographic Solutions' website was not working Thursday morning. The Florida-based company has said its clients include more than 35 states and territories.

Some state-run job seeking sites were also taken offline because of the attack, including Tennessee's. Florida said it was temporarily waiving a job search requirement for those receiving unemployment payments. Texas created a new website for its job seekers with links to popular work search sites such as LinkedIn.

Nebraska said Geographic Solutions indicated that no user's personal data was compromised. Florida said there were no indications any of its state systems were breached.

Bailey, the Tennessee lawmaker, said the state's labor department needs a back-up plan, "so they are not completely dependent on a system proven to be unreliable." He said the state should do "whatever it takes" to get people their unemployment benefits now and streamline the process to update the system with money set aside by state lawmakers.

The length of the potential outage is unknown. Texas said it anticipates its job-search sites to remain offline until early next week.

State governments, as well as their contractors, are often targets of cyber criminals. Nigerian online scam artists were particularly active in

stealing increased unemployment aide at the peak of the coronavirus pandemic.

Ransomware attacks, in which criminals encrypt victims' data and demand payment to return them to normal, continue to cause havoc on digital systems that provide critical government services. A recent ransomware attack on Costa Rica's government caused teachers to go unpaid and caused chaos in the country's health care system.

Last year, cybercriminals launched ransomware attacks in the U.S. that forced the shutdown of an oil pipeline that supplies the East Coast, halted production of the world's largest meat-processing company and compromised a major software company that has thousands of customers around the world.

Despite prioritizing the problem, the U.S. government has had little luck holding major ransomware actors accountable. Many operate in or near Russia with impunity.

Allan Liska, an intelligence analyst at the cybersecurity firm Recorded Future, said an attack affecting those who have lost their jobs from obtaining unemployment benefits is a stark reminder of the huge effects cybercrime can have.

"The people who will be most adversely hurt by this are those with the fewest resources," he said.