Cyberattack shuts down Colorado public defender's office

February 13 2024, by Shelly Bradbury, The Denver Post

Credit: CC0 Public Domain

A cyberattack on the Office of Colorado State Public Defender has forced the office to shut down its computer network, locking public defenders across the state out of critical work systems.

Colorado public defenders do not have access to their work computers, are unable to access court dockets or court filings and can't do any significant work for clients in court, according to internal emails reviewed by The Denver Post.

Office spokesman James Karbach confirmed the breach in a statement Monday, saying officials "recently became aware that some data within our computer system was encrypted by malware."

Karbach did not say how long the public defender's office expects to be shut down or when the attack happened, but emails sent to public defenders indicate the statewide office is effectively non-operational and the outage could last as long as a week.

The "cybersecurity incident" was underway by about 11 a.m. Friday, according to an emailed notice sent from the Colorado Judicial Department's Information and Technology Service's to judges and judicial personnel. The notice indicates that the cyberattack does not pose a threat to the wider court system.

"As a preventative measure, we temporarily disabled our computer network and are working to safely and securely bring systems back online," Karbach said. "Our operations will be limited while the network is offline."

In court Monday morning, public defenders asked to postpone hearings again and again.

"Given the malware with the state public defender, I can't access my files," public defender Amanda Miller said in Adams County District Court as she asked to push a hearing back for a month.

"I'm not allowed to use my computer," public defender Jennifer Chu said

in the same courtroom a few minutes later as she asked to postpone a sentencing.

"I feel like we are going to be doing a lot of this this week," Adams County District Court Judge Jeffrey Smith told Chu. "Let's get you a new date."

The judge later warned another defendant that the computer system outage was expected to last a week.

The wider court system is "fully operational," Colorado Judicial Department spokesman Rob McCallum said.

"Our systems are not impacted by the Public Defender's system breach," he said in a statement. "…As always, we are monitoring our network for any anomalies."

Ransomware attacks are common

The limited information that officials have put out about the cyberattack on the public defender's office suggests the agency was hacked with ransomware, said Steve Beaty, chair of the computer sciences department at Metropolitan State University of Denver, though he cautioned that he is not involved with the incident.

Ransomware attacks are common, he said. In the last few years in Colorado, such attacks have targeted Regis University, the cities of Lafayette and Wheat Ridge, the Colorado Department of Transportation and others.

Attackers use malware to hold an organization's data hostage, Beaty said, then demand a payment in cryptocurrency in order for organizations to regain access to that data. Both public agencies and private businesses

have been targeted in a steady stream of ransomware attacks since about 2013, he said.

"It's a crime that essentially is relatively easy, in the grand scheme of things, to get away with," Beaty said.

About half of victimized organizations pay the ransom, Beaty said. The city of Lafayette forked over $45,000 to ransomware attackers in 2020, and Regis University paid an undisclosed amount of ransom that same year. Wheat Ridge and the Colorado Department of Transportation did not pay their attackers, but spent $1.5 million restoring their systems in 2018.

Whether targeted companies pay depends on the scale of the attack, the company's insurance and the quality of backed-up data, Beaty said. The ransomware attackers often steal a target's financial data first, and know exactly how much a company is likely to pay to retrieve the lost data, he added.

"Essentially it is less expensive to pay the ransomware than to try to bring back all the data from backups," Beaty said.

The malware that powers the cyberattacks is typically delivered into a system either when a person clicks a bad link, often in an emailed phishing attempt, or by exploiting a software bug, Beaty said.

"Very few organizations are immune to this," he said. "…The most important thing is to keep your systems up to date, keep them patched, make sure the known exploits are being fixed, that your firewalls are up to date, that your software on devices is up to date," he said, adding that quality backups are also essential.

"So that when—not if—when we are attacked, we have the ability of

going back and starting fresh a day ago, an hour ago, a week ago."