Cyber attack causes chaos in Costa Rica government systems

April 22 2022, by Javier Córdoba and Christopher Sherman

Credit: Pixabay/CC0 Public Domain

Nearly a week into a ransomware attack that has crippled Costa Rican government computer systems, the country refused to pay a ransom as it struggled to implement workarounds and braced itself as hackers began

publishing stolen information.

The Russian-speaking Conti gang claimed responsibility for the attack, but the Costa Rican government had not confirmed its origin.

The Finance Ministry was the first to report problems Monday. A number of its systems have been affected from tax collection to importation and exportation processes through the customs agency. Attacks on the social security agency's human resources system and on the Labor Ministry, as well as others followed.

The initial attack forced the Finance Ministry to shut down for several hours the system responsible for the payment of a good part of the country's public employees, which also handles government pension payments. It also has had to grant extensions for tax payments.

Conti had not published a specific ransom amount, but Costa Rica President Carlos Alvarado said, "The Costa Rican state will not pay anything to these cybercriminals." A figure of $10 million circulated on social media platforms, but did not appear on Conti's site.

Costa Rican businesses fretted over confidential information provided to the government that could be published and used against them, while average citizens worried that personal financial information could be used to clean out their bank accounts.

Christian Rucavado, executive director of Costa Rica's Exporters Chamber, said the attack on the customs agency had collapsed the country's import and export logistics. He described a race against the clock for perishable items waiting in cold storage and said they still didn't have an estimate for the economic losses. Trade was still moving, but much more slowly.

"Some borders have delays because they're doing the process manually," Rucavado said. "We have asked the government for various actions like expanding hours so they can attend to exports and imports."

He said normally Costa Rica exports a daily average of $38 million in products.

Allan Liska, an intelligence analyst with security firm Recorded Future, said that Conti was pursuing a double extortion: encrypting government files to freeze agencies' ability to function and posting stolen files to the group's extortion sites on the dark web if a ransom wasn't paid.

The first part can often be overcome if the systems have good backups, but the second is trickier depending on the sensitivity of the stolen data, he said.

Conti typically rents out its ransomware infrastructure to "affiliates" who pay for the service. The affiliate attacking Costa Rica could be anywhere in the world, Liska said.

A year ago, a Conti ransomware attack forced Ireland's health system to shut down its information technology system, cancelling appointments, treatments and surgeries.

Last month, Conti pledged its services in support of Russia's invasion of Ukraine. The move angered cybercriminals sympathetic to Ukraine. It also prompted a security researcher who had long been surveilling Conti to leak a massive trove of internal communications among some Conti operators.

Asked why Central America's most stable democracy, known for its tropical wildlife and beaches, would be a target of hackers, Liska said the motivation usually has more to do with weaknesses. "They're looking

for specific vulnerabilities," he said. "So the most likely explanation is that Costa Rica had a number of vulnerabilities and one of the ransomware actors discovered these vulnerabilities and was able to exploit it."

Brett Callow, a ransomware analyst at Emsisoft, said he looked at one of the leaked files from the Costa Rican finance ministry and "there doesn't seem to be much doubt that the data is legit."

On Friday, Conti's extortion site indicated it had published 50% of the stolen data. It said it included more than 850 gigabytes of material from Finance Ministry and other institutions' databases. "This is all ideal for phishing, we wish our colleagues from Costa Rica good luck in monetizing this data," it said.

That seemed to contradict Alvarado's assertion that the attack was not about money.

"My opinion is that this attack is not a money issue, but rather looks to threaten the country's stability in a transition point," he said, referring to his outgoing administration and the swearing in of Costa Rica's new president May 8. "They will not achieve it."

Alvarado did allude to the possibility that the attack was motivated by Costa Rica's public rejection of Russia's invasion of Ukraine. "You also can't separate it from the complex global geopolitical situation in a digitalized world," he said.