Ransomware gang threatens to overthrow Costa Rica government

May 16 2022, by Javier Córdoba

Presidential candidate Rodrigo Chaves greets supporters as he arrives to a polling station during a presidential runoff election in San Jose, Costa Rica, April 3, 2022. Chaves, who won the election, declared a state of emergency over a ransomware attack as soon as he was sworn in early May 2022. Credit: AP Photo/Carlos Gonzalez, File

A ransomware gang that infiltrated some Costa Rican government computer systems has upped its threat, saying its goal is now to overthrow the government.

Perhaps seizing on the fact that President Rodrigo Chaves had only been in office for a week, the Russian-speaking Conti gang tried to increase the pressure to pay a ransom by raising its demand to $20 million.

Chaves suggested Monday in a news conference that the attack was coming from inside as well as outside Costa Rica.

"We are at war and that's not an exaggeration," Chaves said. He said officials were battling a national terrorist group that had collaborators inside Costa Rica.

Chaves also said the impact was broader than previously known, with 27 government institutions, including municipalities and state-run utilities, affected. He blamed his predecessor Carlos Alvarado for not investing in cybersecurity and for not more aggressively dealing with the attacks in the waning days of his government.

In a message Monday, Conti warned that it was working with people inside the government.

"We have our insiders in your government," the group said. "We are also working on gaining access to your other systems, you have no other options but to pay us. We know that you have hired a data recovery specialist, don't try to find workarounds."

Despite Conti's threat, experts see regime change as a highly unlikely—or even the real goal.

"We haven't seen anything even close to this before and it's quite a

unique situation," said Brett Callow, a ransomware analyst at Emsisoft. "The threat to overthrow the government is simply them making noise and not to be taken too seriously, I wouldn't say.

"However, the threat that they could cause more disruption than they already have is potentially real and that there is no way of knowing how many other government departments they may have compromised but not yet encrypted."

Conti attacked Costa Rica in April, accessing multiple critical systems in the Finance Ministry, including customs and tax collection. Other government systems were also affected and a month later not all are fully functioning.

Chaves declared a state of emergency over the attack as soon as he was sworn in last week. The U.S. State Department offered a $10 million reward for information leading to the identification or location of Conti leaders.

Conti responded by writing, "We are determined to overthrow the government by means of a cyber attack, we have already shown you all the strength and power, you have introduced an emergency."

The gang also said it was raising the ransom demand to $20 million. It called on Costa Ricans to pressure their government to pay.

The attack has encrypted government data and the gang said Saturday that if the ransom wasn't paid in one week, it would delete the decryption keys.

The U.S. State Department statement last week said the Conti group had been responsible for hundreds of ransomware incidents during the past two years.

"The FBI estimates that as of January 2022, there had been over 1,000 victims of attacks associated with Conti ransomware with victim payouts exceeding $150,000,000, making the Conti Ransomware variant the costliest strain of ransomware ever documented," the statement said.

While the attack is adding unwanted stress to Chaves' early days in office, it's unlikely there was anything but a monetary motivation for the gang.

"I believe this is simply a for-profit cyber attack," Callow, the analyst said. "Nothing more."