Son of Conti: Ransomware tries its hand at politics

By Dina Temple-Raston

Published: 2023-01-12 · Archived: 2026-04-05 16:48:21 UTC

It has been a busy spring for the Russian-speaking ransomware group Conti.

After an unprecedented leak of its internal chat logs earlier in the year that had experts predicting the group's demise, Conti, or at least some subset of it, came back with a vengeance.

In April it attacked Costa Rica, hacking into dozens of its government agencies and encrypting key servers at the Ministry of Finance, known as the Ministerio de Hacienda. Then, a month later, another ransomware group called HIVE took aim at the nation's health services – canceling schedules and erasing medical records. (Researchers are divided on whether Conti, infamous for its hacks on health services during the pandemic, played a hand in that operation as well.)

Costa Rica's new President Rodrigo Chaves declared a national state of emergency in May, marking the first time a national leader responded to a cyberattack the same way they might respond to a military attack or natural disaster.

"We are at war and that is not an exaggeration," Chaves told reporters days after taking office.

Conti doubled down: "We are determined to overthrow the government by means of a cyberattack," they said. "We have already shown you all the strength and power."

Conti is thought to have shut down the last of its public servers this week. But no one expects them to go away completely. The attack on Costa Rica has raised the specter of ransomware actors changing direction and the concern is that the next generation of ransomware attacks – or the next generation of Conti, the Son of Conti – will focus not just on money but on politics.

Click Here spoke with Jorge Mora, Costa Rica's former director of the Ministry of Science, Innovation, Technology and Telecommunications (MICIT) and Mario Robles is the CEO and founder of White Jaguars, a Costa Rican cybersecurity company that helped the San José government respond to the attack.

The interview has been edited and condensed for clarity.

CLICK HERE: Mr. Mora, you were with MICIT when the attack happened… what went through your mind you realized Conti had targeted you?

JORGE MORA: I was very worried. When I saw it was Conti, the same group that had attacked other countries and other institutions around the world, I was very worried. In the initial stages of the attack, Costa Rica's Finance Ministry told us they had it under control, but it was clear they didn't. Conti started to encrypt the ministry's data and we struggled to understand the real impact.

MARIO ROBLES: Of course we knew about Conti and there were some alerts of potential ransomware attacks here in Costa Rica. But people had the sense it couldn't happen here.

CH: Jorge, you left your post on May 7, just before the President Rodrigo Chaves took office. He declared a national emergency in response to the attacks by Conti. Was that the right move?

JM: Under the previous administration, we asked what's the signal we're sending to the international community by declaring a national emergency. We coordinated a lot with other countries, like the United States, Spain, and Israel. We also worked with the private sector to increase the cybersecurity systems. At this moment, I don't think the national emergency was necessary.

CH: What lessons were learned from this attack by Conti?

JM: Maybe the first lesson is the importance of living in a connected and digital world. There are new security challenges. The dangers are in your house and your office because you enter a digital world. Both in the private and public sectors, we need to increase the budget in Costa Rica to protect digital systems and boost education about cyber security because people don't know how to protect themselves online.

MR: The problem is more fundamental. Costa Rica doesn't have enough resources for enforcing or auditing institutions. So we're talking about a group of people, less than five people handling cybersecurity controls in more than 300 institutions. That's crazy.

CH: Before Conti went after Costa Rica, how prepared do you think the country was for this kind of attack?

JM: We worked a lot with the European Union in cybersecurity training, and with IT teams in the public sector over the last couple of years. So, we always told the Costa Rican government that these kinds of incidents were a probability, and we need to work to reduce the risk but they didn't listen.

CH: Hackers struck again in May, but this time they targeted the Costa Rican Social Security fund, which manages the country's public health system and pension checks. Some people think Conti was involved or at least worked with another group to launch that attack… what was your reaction when that news came, Mario?

MR: To be honest, that's the attack that scares me the most because it affected the Costa Rican people directly. At the moment, for instance, you don't have a way to know your healthcare records. People say they were waiting for surgery for more than a year. And right now the appointment schedule is just lost. Medical records are blocked or are not available. So there is no way that doctors can see the historical information for treating a new patient. I think that's critical.

CH: So why Costa Rica?

JM: One hypothesis is that Costa Rica had the ability to pay and it was vulnerable. There is also reason to believe that Conti had shifted its focus to the region. We think they had been in contact with other cyber gangs in the region… particularly in Peru… and we think that played a role.

MR: I think it is about relationships and geo-politics. Costa Rica may have also been targeted because of its strong ties to the United States. Many U.S. companies are here and we've been very public about encouraging the nation

to have a strong relationship with the U.S. So, for a Russian group trying to hit a small country in Central America, it makes sense that we would be targeted and that it would be us.

CH: Do you think we're seeing the beginning of a new trend – country extortion instead of more run-of-the-mill ransomware attacks? Do you think Costa Rica will be hit again?

JM: Yes, I think we are going to have more incidents in the future. At this moment, Costa Rica doesn't have enough of a budget to protect all the institutions, and we have a digital divide in public situations. So, these two situations make us vulnerable. We need to try to work to reduce this risk as much as possible. We need to prepare with the backups, communication and cybersecurity strategy plans. We also need to increase international collaboration. For example, the United States helped us a lot by offering a $10 million reward [for any information leading to the arrest of leaders of Conti].

MR: If we get hit again, I don't think it's going to be shocking for the people here. They're kind of getting used to it. It's bad to say that, but I think it's what's happening. They've gotten kind of numb.

CH: Do you think Conti still exists?

MR: Um. I think they do. They just say they are disbanding the group, but I'm, I'm not completely sure…I don't think they're going to stop this. So they're going to come back with another name. I don't think they're going to stop.

Dina Temple-Raston

is the Host and Managing Editor of the Click Here podcast as well as a senior correspondent at Recorded Future News. She previously served on NPR's Investigations team focusing on breaking news stories and national security, technology, and social justice and hosted and created the award-winning Audible Podcast "What Were You Thinking."

Sean Powers

is a Senior Supervising Producer for the Click Here podcast. He came to the Recorded Future News from the Scripps Washington Bureau, where he was the lead producer of "Verified," an investigative podcast. Previously, he was in charge of podcasting at Georgia Public Broadcasting in Atlanta, where he helped launch and produced about a dozen shows.
