# Costa Rica chaos a warning that ransomware threat remains

June 17 2022, by Alan Suderman and Ben Fox

Costa Rica President Rodrigo Chaves Robles smiles during the opening plenary session at the Summit of the Americas June 9, 2022, in Los Angeles. Costa Rica has been reeling from unprecedented ransomware attacks disrupting everyday life in the Central American nation for the last two months. Credit: AP Photo/Marcio Jose Sanchez, File

Teachers unable to get paychecks. Tax and customs systems paralyzed. Health officials unable to access medical records or track the spread of COVID-19. A country's president declaring war against foreign hackers saying they want to overthrow the government.

For two months now, Costa Rica has been reeling from unprecedented ransomware attacks disrupting everyday life in the Central American nation. It's a situation raising questions about the United States' role in protecting friendly nations from cyberattacks when Russian-based criminal gangs are targeting less developed countries in ways that could have major global repercussions.

"Today it's Costa Rica. Tomorrow it could be the Panama Canal," said Belisario Contreras, former manager of the cybersecurity program at the Organization of American States, referring to a major Central American shipping lane that carries a large amount of U.S. import and export traffic.

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.

The Biden administration responded with a whole of government action that included included diplomatic, law enforcement and intelligence efforts designed to put pressure on ransomware operators.

Since then, ransomware gangs have shied away from "big-game" targets in the U.S. in pursuit of victims unlikely to provoke a strong response by the U.S.

"They're still prolific, they're making enormous amounts of money, but

they're just not in the news everyday," Eleanor Fairford, a deputy director at the UK's National Cyber Security Centre, said at a recent U.S. conference on ransomware.

Tracking trends of ransomware attacks, in which criminals encrypt victims' data and demand payment to return them to normal, is difficult. NCC Group, a UK cybersecurity firm that tracks ransomware attacks, said the number of ransomware incidents per month so far this year has been higher than it was in 2021. The company noted that the ransomware group CL0P, which has aggressively targeted schools and health care organizations, returned to work after effectively shutting down for several months.

But Rob Joyce, the director of cybersecurity at the National Security Agency, has said publicly that there's been a decrease in the number of ransomware attacks since Russia's invasion of Ukraine thanks to increased heightened concerns of cyberattacks and new sanctions that make it harder for Russian-based criminals to move money.

The ransomware gang known as Conti launched the first attack against the Costa Rican government in April and has demanded a $20 million payout, prompting the newly installed President Chaves Robles to declare a state of emergency as the tax and customs offices, utilities and other services were taken offline. "We're at war and this is not an exaggeration," he said.

Later, a second attack, attributed to a group known as Hive knocked out the public health service and other systems. Information about individual prescriptions are offline and some workers have gone weeks without their paycheck. It's caused significant hardship for people like 33-year-old teacher Alvaro Fallas.

"I live with my parents and brother and they are depending on me," he

said.

In Peru, Conti has also attacked the country's intelligence agency. The gang's darkweb extortion site posts purportedly stolen documents with the agency's information, like one document market "secret" that details coca-eradication efforts.

Experts believe developing countries like Costa Rica and Peru will remain particularly ripe targets. These countries have invested in digitizing their economy and systems but don't have as sophisticated defenses as wealthier nations .

Costa Rica has been a longtime stable force in a region often known for upheaval. It has a long established democratic tradition and well-run government services.

Paul Rosenzweig, a former top DHS official and cyber consultant who is now a legal resident of Costa Rica, said the country presents a test case for what exactly the U.S. government owes its friendly and allied governments who fall victim to disruptive ransomware attacks. While an attack on a foreign country may not have any direct impact on U.S. interests, the federal government still has a strong interest in limiting the ways in which ransomware criminals can disrupt the global digital economy, he said.

"Costa Rica is a perfectly good example because it's the first," Rosenzweig said. "Nobody has seen a government under assault before."

So far, the Biden administration has said little publicly about the situation in Costa Rica. The U.S. has provided some technical assistance through its Cybersecurity and Infrastructure Security Agency, via an information-sharing program with nations around the world. And the State Department has offered a reward for the arrest of members of

Conti.

Eric Goldstein, the executive assistant director for cybersecurity at CISA, said Costa Rica has a computer emergency response team that had an established relationship with counterparts in the U.S. before the incidents. But his agency is expanding its international presence by establishing its first overseas attache position in the U.K. It plans others in as-yet unspecified locations.

"If we think about our role, CISA and the US government, it is intrinsically of course to protect American organizations. But we know intuitively that the same threat actors are using the same vulnerabilities to target victims around the world," he said.

Conti is one of the more prolific ransomware gangs currently operation and has hit over 1,000 targets and received more than $150 million in payouts in the last two years, per FBI estimates.

At the start of invasion of Ukraine, some of Conti's members pledged on the group's dark web site to "use all our possible resources to strike back at the critical infrastructures of an enemy" if Russia was attacked. Shortly afterward, sensitive chat logs that appear to belong to the gang were leaked online, some of which appeared to show ties between the gang and the Russian government.

Some cyber threat researchers say Conti may be in the middle of a rebranding, and its attack on Costa Rica may be a publicity stunt to provide a plausible story for the group's demise. Ransomware groups that receive lots of media attention often disappear, only for its members to pop back up later operating under a new name.

On its darkweb site, Conti has denied that's the case and continues to post victims' files. The gang's most recent targets include a city parks

department in Illinois, a manufacturing company in Oklahoma and food distributor in Chile.