BBC – 19.05.2022

President Rodrigo Chaves says Costa Rica is at war with Conti hackers

Президент Родріго Чавес Роблес заявив, що Коста-Ріка воює з хакерами Conti

Президент Коста-Ріки Родріго Чавес Роблес каже, що його країна перебуває у стані війни, оскільки кіберзлочинці спричиняють серйозні порушення в IT-системах численних урядових міністерств. Р. Чавес Роблес сказав, що хакери проникли в 27 державних установ, включаючи муніципалітети та державні комунальні підприємства. Картель програм-вимагачів Conti, який, як вважають, керується з росії, підвищив вимоги щодо викупу до 20 млн дол. Зловмисники розмістили в мережі заклик до коста-ріканців «вийти на вулицю і вимагати оплати».
https://www.bbc.com/news/technology-61323402

The president of Costa Rica says his country is "at war", as cyber-criminals cause major disruption to IT systems of numerous government ministries.

Rodrigo Chaves said hackers infiltrated 27 government institutions, including municipalities and state-run utilities.

The Conti ransomware cartel, which is thought to be run from Russia, has upped its ransom demand to $20m (£16m).

The criminals posted an appeal online to Costa Ricans to "go out on the street and demand payment".

Mr Chaves held a press conference on Monday to outline his "Plan for Implementation of Cyber-security Measures".

He gave no indication that he was planning on paying the ransom, in spite of growing disruption to government departments.

On Wednesday, the Costa Rican Treasury told civil servants that the hack had affected automatic payment services. It warned that they would not be paid on time, and would need to apply for their salaries by email, or on paper by hand.

The ministry said: "Due to the temporary downturn of the institutional systems, the service of issuing certificates regarding the amounts of salaries owed to the civil servants of the Central Administration is suspended.

"All applications received via email or in the windows of the National Accountancy will be attended to once systems are restored."

According to the government, the attacks also affected the country's foreign trade by hitting its tax and customs systems.

The president, who was elected fewer than two weeks ago, declared the incident a "national emergency" and has repeatedly blamed his predecessor for not taking the cyber-attack seriously enough.

The hackers were demanding $10m when the attack started last month.

A government website says that a declaration of a state of emergency allows it, in exceptional cases, to undertake on its own some procedures that would normally require legislative approval.

For example, it allows the government to allocate public funds to deal with an emergency, without previous legislative consent.

"The attack being experienced by Costa Rica at the hands of cyber-criminals, cyber-terrorists, is declared a national emergency," Mr Chavez said, according to local media.

"We are signing this decree, precisely, to declare a state of national emergency across the entire public sector of the Costa Rican state, and allow our society to respond to those attacks as criminal actions."

The Conti hacking group has posted more than 600 gigabytes of government data online, and is threatening to publish more.

It has also posted on its darknet website that it will delete the decryption keys needed to restore the government's computer systems to normality, unless it is paid within a week.

"There is less than a week left when we destroy your keys, we are also working on gaining access to your other systems, you have no other options but to pay us," it threatened.

On its darknet website, Conti writes to the Costa Rican government: "You're forcing us to use terrible methods..."

And "terrible" is the word many cyber-security researchers are using to describe these new tactics the hackers are using to put pressure on the Costa Rican government to pay.

In the past, ransomware crews have attacked public bodies and local governments, but it is rare to see such a disruptive attack on a state.

It's also unprecedented to see such aggressive threats and direct appeals to Costa Ricans to "take to the streets".

The hackers also claim to have operatives on the inside of government - which may be unlikely but further piles the pressure on the president.

In some ways it all reads like desperation.

Conti has probably put a lot of work into its attack and it looks like it may come away empty-handed.

But it is also another terrible reminder of the power criminal hackers can wield, even against governments.

Conti is a prolific Russian speaking ransomware group responsible for many high-profile hacks.

In May 2021, the group carried out a "catastrophic hack" of the Irish Health Service.

On 6 May, the US offered a $10m reward for information about the group's leadership.

It blamed Conti for the cyber-attacks which hit Costa Rica.

Cyber-security researcher Maya Horowitz, of Check Point, says Costa Rica is not the only country to be targeted by criminals, who may be put off US organisations because of pressure from the authorities there.

"Recently we have seen two massive ransomware attacks in Costa Rica and Peru, both reportedly executed by the infamous Conti ransomware gang.

"Based on our latest research, Conti's extortion planning is very focused and based on the ability of the victim to pay," she added.

Mrs Horowitz said the research also suggested that the financial impact of a ransomware attack is "seven times higher than the initial extortion demand, but we assume in the case of a wide attack on a government like we see here, the total costs will be considerably more".