- Currently Conti is conducting a wide extortion operation against two governments in Latin America – Costa Rica and Peru
- It is unprecedented for a country to declare a state of war with a cybercriminal group
- Attacks by Conti on sovereign countries depict the growing power of organized cybercrime groups

An unprecedented event has occurred in Costa Rica. On May 12, the country's president declared a state of national emergency. Days later, he announced that the country is at war; a war against a cybercrime group – Conti. This took place after the Conti group breached and encrypted at least 27 of Costa Rica's governmental agencies. Moreover, while the government decided not to pay the ransom, the group declared its goal to overthrow the government of Costa Rica and called for its citizens to go to the streets and change the government. This probably started as a regular ransomware attack, but it quickly turned into a new type of event with significant financial and geopolitical consequences. In this case, both Conti and Costa Rica brought the US to the stage, which perfectly fits the group's pro – Russian agenda. Even if all those events are just a smoke screen for rebuilding Conti's operations, the group has already made a mark that country extortion is possible, and a cybercrime group can be a player in a geopolitical area.

In this blog post, Check Point Research (CPR) looks into Conti's increased activity since the start of the Ukraine- Russia war, which came to its peak with "country extortion" against the governments of Costa Rica and Peru.

## Webinar: Ransomware or ransom-war? Country extortion-The Costa Rica story

## Conti Group in 2022 – Non-Stop Targeting and Increased Public Aggression

Since the groups emergence in 2020, Conti has taken the place as a leader of the underground ransomware market and is known as one of the most prolific and innovative groups out there. They have accumulated more than 800 victims, mostly large companies and corporations with millions of dollars in revenue. The Conti ransomware group is well known for bringing double and triple extortion tactics against its victims to a state of near perfection. Check Point's latest research showed that Conti is more than just a cybercrime group, but an organized, hierarchical and structured tech company. While some ransomware groups reduced their activity due to the Ukraine – Russia war and the western sanctions on Russia, we saw an opposite phenomenon from the Conti group. Despite the major leak Conti suffered at the end of February, we see that during the months of March – April 2022 Conti had significantly increased the number of its victims compared to January – February; probably as a smoke screen to its reorganization efforts.

Conti Victims in 2022 according to their shame blog

## "Country Extortion" against Costa Rica

In the last month, Conti not only expanded the number of its victims, but also extended the type of victims. In a bold move, the group decided to attack and extort entire countries. In the past, ransomware groups have attacked different governmental entities around the world, those were mostly specific, tactical attacks on municipal level entities and not wide attacks on critical governmental services. Conti is conducting a wide extortion operation against two governments in Latin America – Costa Rica and Peru. Both incidents are developing attacks that started with a small compromise of one agency in each country, and quickly expanded to country wide extortions.

Moreover, those attacks went beyond the scope of a purely financially motivated attack, and have now become geopolitical events. The Costa Rican government declaring a national emergency and stating they are at war with Conti, has led the US government to intervene in the situation and support Costa Rica. This is an unprecedented situation when a country declares they are at war with a cybercriminal group.

As a result of the attack against Costa Rica, which involved 27 governmental agencies, the Costa Rican president declared on May 12th a state of national emergency.

The "country extortion" of Costa Rica has various unique features:

1. A coordinated attack by a cybercrime group on a large number of governmental entities of one country causing disruption of critical services such as customs, export of goods and automatic payment services for civil servants.
2. "Triple Extortion" – the cybercriminals are using the people of Costa Rica as a means of pressure against the government, in order to persuade them to pay the ransom.
3. Intervention in one country's democracy – Conti claims that their goal is to overthrow democratically elected government and encourage the people of Costa Rica to go out to the streets and demonstrate against the government.

This quickly escalating cyber event has evolved into a wide geopolitical event. It happened when on the one hand, Costa Rica asked for support from the US and the US state department then offered a $10,000,000 reward for information on Conti's leaders. On the other hand, the rhetoric of the Conti group around the Costa Rican extortion started to involve the US and President Biden, and not just Costa Ricans.

The event received a lot of positive attention in the Russian speaking underground and could potentially lead to further ransomware groups utilizing the same concepts against other countries and in different geopolitical circumstances. One of the most reputable members of the Russian Underground aggressively reacted to the US intervention, saying that Americans should pray that the events of May — June 2021 won't happen again, alluding to the Colonial Pipeline ransomware attack.

Reaction of a reputable member of the Russian underground to the reward offered by the US on Conti group members

Analysis of some of Conti's posts on the shame website regarding the attack on Costa Rica depicts an unprecedented rhetoric of a cybercrime group against countries and governments. It started with Costa Rica but continued to even harsher and ruder language towards the US and President Biden.

The following is the full chain of the posts by Conti about the attack:

1. April 17th — The attack started as a regular ransomware attack with a ransom note about the Ministry of Finance of Costa Rica

2. April 20th — Conti group explains the full scope of their access to the Ministry of Finance of Costa Rica and claims that they already have initial access to a variety of other ministries' databases and private companies in Costa Rica.

3.April 21st — Conti publishes the database of the Costa Rican Ministry of Finance

4.April 22nd — Conti threatens that after Costa Rica asked the US to assist, they will now focus on attacking large companies within Costa Rica

5.April 27th — Conti escalates its rhetoric towards Costa Rica, while understanding that the new government is not ready to pay the requested ransom.

6.April 27th — Conti escalates its rhetoric towards Costa Rica, while understanding that the new government is not ready to pay the requested ransom.

7.May 9th — Conti starts a harsh anti-US rhetoric and claims that in the future it will execute even larger "country extortion" attacks than the one against Costa Rica, with a more serious team.

8.May 14th — Conti exercised a triple extortion strategy, where it asked the citizens of Costa Rica to demonstrate against their government so they would pay, and suggested replacing the government.

9. May 14th — Conti claims that its official goal now is to overthrow the government of Costa Rica

10.May 16th — Conti claims to have insiders within the Costa Rican government and that if the ransom will not be paid within a week, they will destroy the decryption keys.

11. May 19th — Conti escalates its rhetoric against the US

12. May 20 — Conti threatens to publish all the data from Costa Rica on Monday, May 23rd

## "Country Extortion" against Peru

Peru is another victim of country extortion by Conti. The public stage of the extortion attack against Peru started on May 7, and currently focuses on two key government entities — Ministry of Finance and General Intelligence Directorate.

Extortion against Peru is a developing incident which is in the early stages compared to the event against Costa Rica. We hope it will be stopped before it reaches the extent of the Costa Rican event.

## How to Protect Against Ransomware

Taking the following best practices can reduce an organization's exposure to ransomware and minimize its impacts:

1. Continuous data backups: The definition of ransomware is explained as malware designed to force a ransom payment as the only way to restore access to the encrypted data. Automated, protected data backups enable an organization to recover from an attack with minimum data loss and without paying a ransom. Maintaining regular backups of data as a routine process is a very important practice to prevent losing data, as well as to be able to recover it in the event of corruption or disk hardware malfunction.

2. Patching: Patching is a critical component in defending against ransomware attacks as cyber-criminals will often look for the latest uncovered exploits in the patches made available and then target systems that are not yet patched. As such, it is critical for organizations to ensure that all systems have the latest patches applied to them, as this reduces the number of potential vulnerabilities within the business for an attacker to exploit.
3. User Authentication: Accessing services like RDP with stolen user credentials is a favorite technique of ransomware attackers. The use of strong user authentication can make it harder for an attacker to make use of a guessed or stolen password
4. Reduce the Attack Surface: With the high potential cost of a ransomware infection, prevention is the best ransomware mitigation strategy. This can be achieved by reducing the attack surface by addressing:

1. 1.
   - Phishing Messages
   - Unpatched Vulnerabilities
   - Remote Access Solutions
   - Mobile Malware

1. Deploy Anti-Ransomware Solution: The need to encrypt all of a user's files means that ransomware has a unique fingerprint when running on a system. Anti-ransomware solutions are built to identify those fingerprints. Common characteristics of a good anti-ransomware solution include:
   - Wide variant detection
   - Fast detection
   - Automatic restoration
   - Restoration mechanism not based on common built-in tools (like 'Shadow Copy', which is targeted by some ransomware variants)
2. Cyber Awareness Training and Education:Ransomware is often spread using phishing emails. Training users on how to identify and avoid potential ransomware attacks is crucial. As many of the current cyber-attacks start with a targeted email that does not even contain malware, but only a socially engineered message that encourages the user to click on a malicious link, user education is often considered as one of the most important defenses an organization can deploy.

## Conclusion

The two attacks by Conti on sovereign countries and the rhetoric they use, depict the growing power of organized cybercrime groups. In these cases, Conti showed not only the power of the technological means (e.g., malware, ransomware, etc.) that they are using, but also the power of information warfare means being implemented by a cybercrime group. Whatever their real reason behind the attacks on Costa Rica and Peru might be, they definitely opened a new chapter in the ransomware eco system.

## Webinar: Ransomware or ransom-war? Country extortion-The Costa Rica story

### Related Articles

Cybersecurity for banks — How Global Banks enable the secure remote workforce

5 Essential Ways to Improve SDLC Security

From Bitcoin to the Metaverse: The current evolution is a revolution

Twisted Panda: Check Point Research unveils a Chinese APT espionage campaign against Russian state-owned defense institutes

Check Point Harmony Mobile Introduces Malicious File Protection

Secure Your Migration to AWS, Part II: The Road to Success

Ransomware cyber-attacks in Costa Rica and Peru drives national response

How the evolution of ransomware has changed the threat landscape

April 2022’s Most Wanted Malware: A Shake Up in the Index but Emotet is Still on Top

Info-stealer Campaign targets German Car Dealerships and Manufacturers