Small Ball in the Global Cyberware; Or, They Got Bugs. We Got Bugs. All God's Chillun Got Bugs Part 1

They got guns
We got guns
All God's chillun got guns

— Bert Kalmar, "This Country's Going to War"
Duck Soup, The Marx Brothers

In researching for interesting facts or events in writing this blog, I occasionally run across an article than causes even an old jaded war horse such as myself to have a real ***WTF?*** moment. My most recent moment of astonishment came when I read the news that the nation of Albania suffered a cyberattack that caused the government of Albania to shut down all of its computers. **Iran had been credited with launching the attack against this small Balkan country**. The **Albanian Daily News**, which bills itself as "The Most Authoritative Albanian Source in English," first reported the attack, **July 17, 2022**, with the following:

> **The National Agency of the Information Society (AKSHI) has informed that they were forced to shut down government systems until the neutralization of the enemy attacks in order to cope with the cyber attacks.**

Of course, to a casual observer to world events, one must wonder what did Albania do to Iran to warrant a crippling cyberattack? Albania was the host nation for an event in July 2022, called, "**Free Iran World Summit.**" That threats had been made to this event caused the US State Department to warn American citizens to avoid the Summit. "**The US government is aware of a potential threat targeting the Free Iran World Summit to be held near Durres.**" Ultimately, the Free Iran conference **was postponed because of the cyberattck.**

And, keeping with times, the nature of the attack was ransomware. The malware that brought down Albanian servers also contained several disk wiping components. It must be remembered that although small, Albania is a NATO member nation. **This prompted researchers for security provider, Mandiant, to note**:

> **The use of ransomware to conduct a politically motivated disruptive operation against the government websites and citizen services of a NATO member state in the same week an Iranian opposition groups' conference was set to take place would be a notably brazen operation by Iran-nexus threat actors.**

This attack on that geopolitical farthing, Albania, follows on an even more devastating attack on that powerhouse of the Caribbean, Costa Rica. It is believed that the Conti Russian ransomware gang began its intrusions into Costa Rican systems in April 11, 2022. **By first compromising the Ministry of Finance, four days later the gang had stolen "672GB of data on April 15 and executing the ransomware."** A set of credentials for the Ministry of Finance were hijacked and used to gain access and launch the attack.

On May 8, 2022, Costa Rica declared a National emergency, as the ransomware spread to all other departments of the government. The government of Costa Rica refused to pay the $10 million ransom that grew to $20 million as the attack continued. To the Costa Rican people it felt much like a foreign invasion — as if Russians forces had landed at the Port of Caldera. And internal subversives were suspected in assisting Conti. **As Costa Rican President Rodrigo Chaves declared**:

> **We're at war and this is not an exaggeration,... The war is against an international terrorist group, which apparently has operatives in Costa Rica. There are very clear indications that people inside the country are collaborating with Conti.**

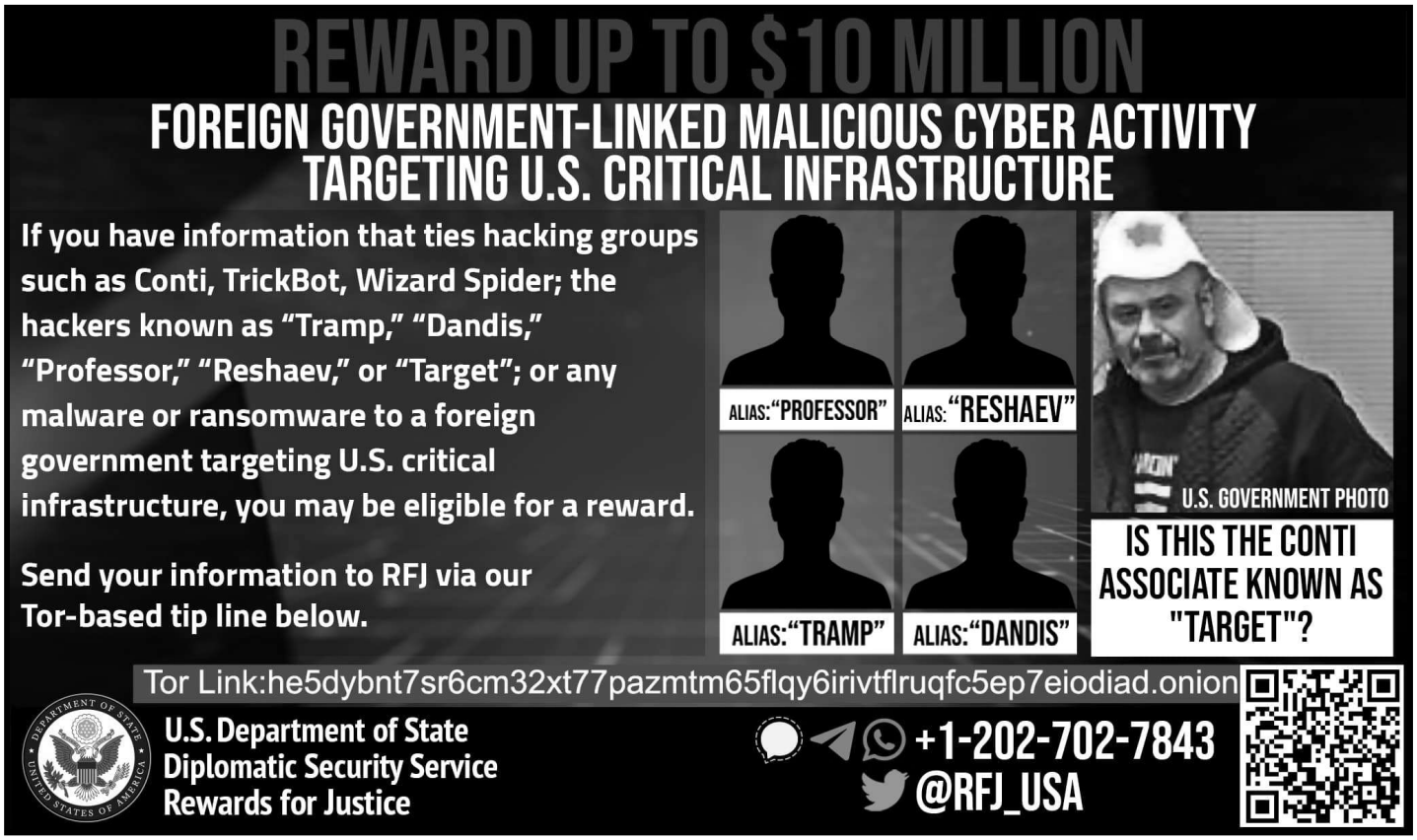
There is a certain symmetry to the two attacks. **Iran and Albania have a long history of conflict**. Most recently, **Albania is the host country for about 3,000 Iranian exiles, a contingent of the People's Mujahedin of Iran, MEK**. **Costa Rica, for its part, has been very supportive of Ukraine in the current conflict. Other security experts think the Conti is simply profit motivated, and believed Costa Rica had the means and ability to pay.**

As of July 21, 2022, the situation in Costa Rica has yet to be resolved. Costa Rica refuses to pay. And so the attack continues, as far as my research shows.

Whatever be the differing motives for the two attacks, when considered together, "**The success of these attacks should concern smaller governments around the world,**" said Allan Liska, an intelligence analyst at Recorded Future. Liska added that gangs like Conti think they are untouchable:

This is going to be an increasingly bigger problem and governments have to take firm action against ransomware actors. These are non-nation-state groups engaging in essentially nation-state-style attacks and there should be appropriate repercussions for these actions.

And experts agree that large scale debilitating attacks against a powerhouse like the United States, although possible, are unlikely, and would probably not have the same devastating consequences as befell Albania and Costa Rica. Less wealthy countries, with less investment in cyber security, will however certainly be likely future targets of ransomware attacks.



US State Department offers $10 million reward for Conti Crooks

"In case you haven't heard before
I think they think we're going to war
I think they think we're going to war

— Bert Kalmar, "This Country's Going to War"
Duck Soup, The Marx Brothers

Back to Top

Gerald Reiff

Back to Top

next post →