First Conti, then Hive: Costa Rica gets hit with ransomware again

By Ofir Ashman

Published: 2022-06-15 · Archived: 2026-04-06 00:25:05 UTC

It must suck dealing with a huge ransomware attack during your first week in office... Sadly, that's exactly what happened to new Costa Rica president Rodrigo Chaves, who declared last month that his country is "at war" with Conti hackers. In mid-April, only a few days after Chavez was chosen to replace previous president Carlos Alvarado Quesada, 27 Costa Rican government systems and institutions were hit with Conti ransomware, including municipalities and state-run utilities. This disrupted various government systems, including those used to oversee exports, pay pensions, and collect taxes.

The blame came quickly, with Chaves claiming that the his predecessor had not invested enough in cybersecurity, nor had he dealt more aggressively with the attacks during his last days in office. While the Costa Rican government refused to pay the ransom, the impatient Conti gang started publishing the stolen government information on its website. Some believe that the publications serve not only as a way to entice a ransom payment, but as a warning sign for other governments, displaying the heavy price of a Conti attack.

But just when news of the attack started to fade out, another Russian ransomware group dubbed Hive joined in, hitting Costa Rica's Social Security system and public health agency. 30 public health system servers were hit with ransomware, Covid-19 test reporting was halted, and computers were shut down to prevent further spread of the ransomware in the network. Some theorize that these two consecutive attacks on the Central American country are related, claiming that Conti group members are involved with Hive, and have separated into smaller groups to evade law enforcement. This makes sense considering the many sanctions posed as a result of Russia's invasion of Ukraine, alongside the Conti gang's public declaration of support towards the invading country.

In Cybersecurity: Effective > Expensive

Is investing more money really the key to better attack prevention? Is aggression in dealing with hackers the best response and remediation tactic? Perhaps not. Cyber security should be effective, not expensive. Unfortunately, marketing in this sector drives security buyers to believe that only expensive solutions will deliver the efficacy they need.

Many security vendors offer feature-packed platforms with shiny interfaces and complex mechanisms that attempt to discover sophisticated threats once they are inside the network. These reactive "enterprise" solutions come with a price tag no one is happy to pay, and are not necessarily the most effective at reducing cyber-risk. For example, if your security solution blocks threats proactively at the gateway, threats can't cause damage, don't lead to a breach, and won't even get detected by the reactive, expensive security controls - because the threat never gets a chance to enter the network.

Over the past decade of our own research, we've found that most attack methods, infection vectors and threat infrastructure are recycled by cyber attackers. Gartner has predicted that over time, "99% of vulnerabilities exploited will continue to be the ones known by security and IT professionals for at least one year". We have seen

thousands of IOCs blocked by ThreatSTOP's solutions being reused for various malicious activity over and over again. ThreatSTOP protects from known threats and newly registered IOCs, providing our customers with an instant 85% reduction in malware infections and help desk tickets. Regardless of the attack type, the vectors, or the variant, the IP addresses and domains cyber criminals use to conduct an attack can only harm your network if your network is allowed to talk to them. This is where proactive security controls like ThreatSTOP really deliver on reducing risk - automating early mitigation tilts the advantage to network defenders by stopping the huge volumes of garden-variety attacks from gaining a foothold in your network, and freeing your skilled people to focus on the other 1% of truly challenging threats.

Not a ThreatSTOP customer yet? Want to see ThreatSTOP instantly eliminate attacks on your network?

Get a Demo
