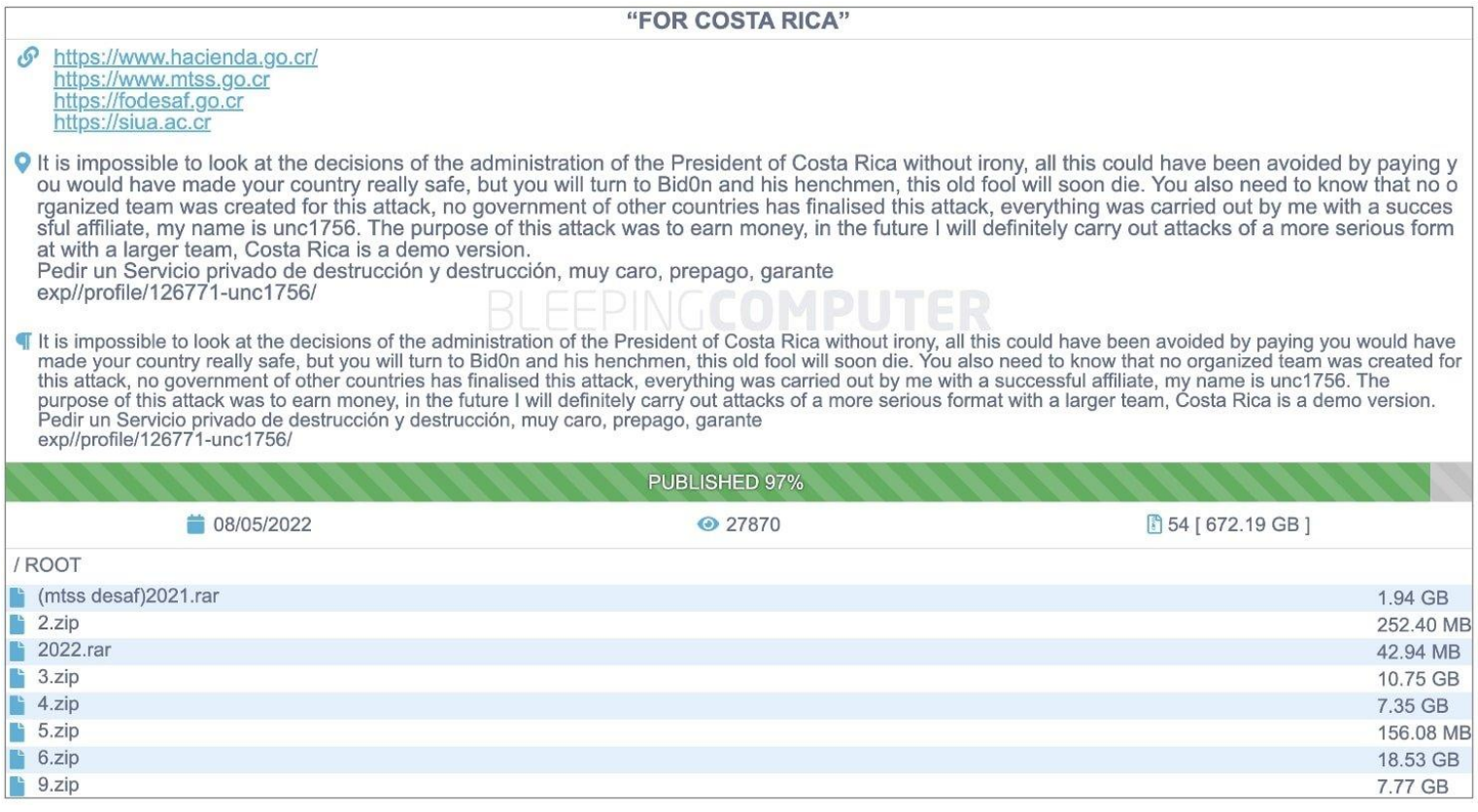
Severity

High

Analysis Summary

May 8, 2022: Costa Rican President Rodrigo Chaves has declared a national cybersecurity emergency following the crippling of the country's government and economy by the Conti ransomware attack. Conti allegedly demanded a $10 million ransom from Costa Rica in exchange for the data from the Ministry of Finance not being released, but the government refused to respond. Researchers also observed that Conti published most of the 672 GB dump containing data belonging to the Costa Rican government agencies.



Conti's leak site lists the following government purportedly affected by the attack: The Costa Rican Finance Minsitry, Ministerio de Hacienda The Ministry of Labor and Social Security, MTSS The Social Development and Family Allowances Fund, FODESAF The Interuniversity Headquarters of Alajuela, SIUA

The Peru MOF — Dirección General de Inteligencia (DIGIMIN) recently added to the list of victims on the Conti ransomware group's Tor leak site. According to the Conti ransomware group, they have stole 9.41 GB of data. The National Directorate of Intelligence is Peru's top intelligence agency which is responsible for national, military, and counterintelligence. The Conti ransomware group has been responsible for hundreds of ransomware outbreaks over the last two years. According to a State Department spokesperson, this group has targeted over 1,000 victims who have paid over $150 million in ransoms till January 2022.

A $15 million reward — To counteract Conti's ransomware attacks on Costa Rica and others, the United States offered a $15 million reward for information leading to identifying and locating the renowned Conti ransomware group's leadership and co-conspirators. A $10 million reward is attainable for the info on Conti leaders' identity and location, also an additional $5 million is available for information leading to the arrest and/or conviction of people who collaborated or tried to engage in Conti ransomware attacks.

Impact

- Information Theft and Cyber Espionage
- Exposure of Sensitive Data
- Unauthorized Access

Remediation

- Logging — Log your eCommerce environment's network activity and web server activity.
- Passwords — Ensure that general security policies are employed including: implementing strong passwords, correct configurations, and proper administration security policies.
- Admin Access — limit access to administrative accounts and portals to only relevant personnel and make sure they are not publicly accessible.

- WAF — Web defacement must be stopped at the web application level. Therefore, set up a Web Application Firewall with rules to block suspicious and malicious requests.
- Patch — Patch and upgrade any platforms and software timely and make it into a standard security policy. Prioritize patching known exploited vulnerabilities and zero-days.
- Secure Coding — Along with network and system hardening, code hardening should be implemented within the organization so that their websites and software are secure. Use testing tools to detect any vulnerabilities in the deployed codes.
- 2FA — Enable two-factor authentication.
- Antivirus — Enable antivirus and anti-malware software and update signature definitions in a timely manner. Using a multi-layered protection is necessary to secure vulnerable assets