Indonesia's central bank confirms ransomware attack, Conti leaks data

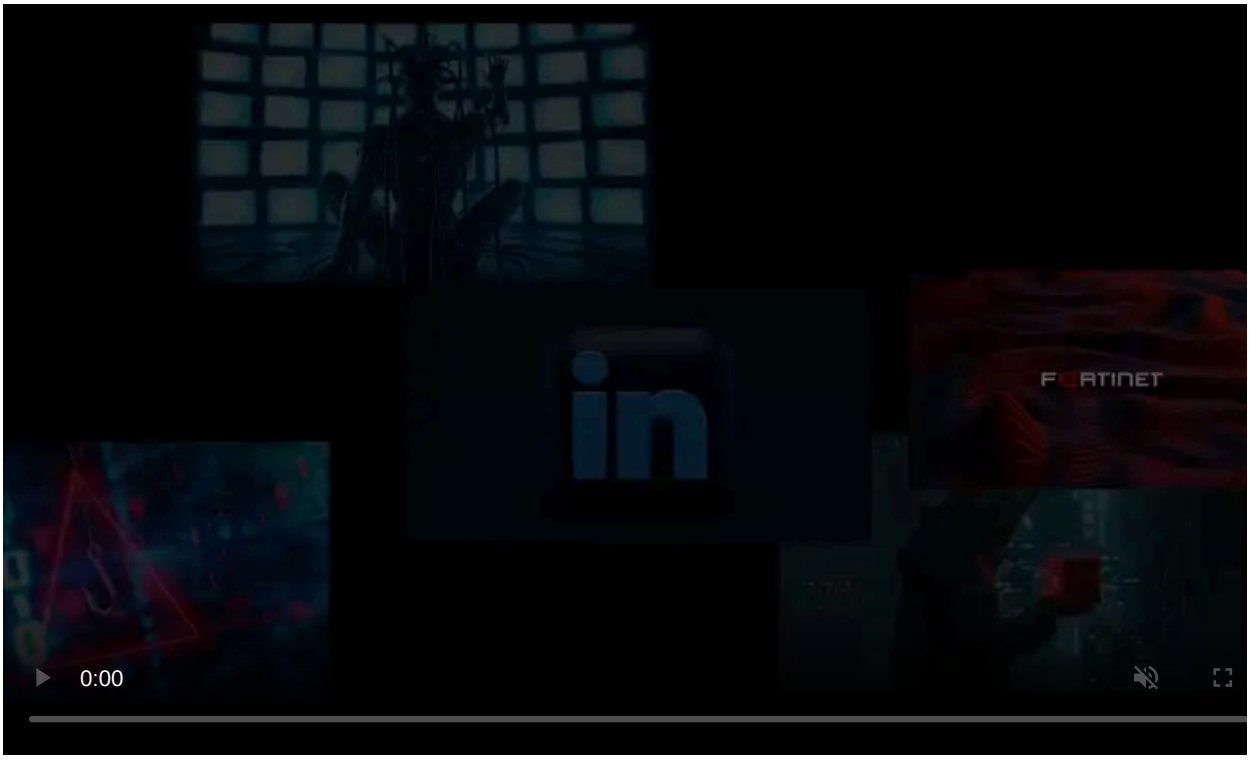
By Sergiu Gatlan

Published: 2022-01-20 · Archived: 2026-04-05 19:41:40 UTC

Bank Indonesia (BI), the central bank of the Republic of Indonesia, has confirmed today that a ransomware attack hit its networks last month.

A Bank Indonesia spokesperson also told BleepingComputer the attack took place last month and that the bank's operations are not disrupted after the incident.

"We would like to inform you that the ransomware harassment has occurred last month. However, Bank Indonesia has conducted comprehensive evaluation for the disruption," BleepingComputer was told.


0:00

"We convince that our operational activities are not disrupted, stay in control, and keep on support public economic services."

During the incident, the attackers stole "non-critical data" belonging to Bank Indonesia employees before deploying ransomware payloads on over a dozen systems on the bank's network, as CNN Indonesia reported.

According to the bank, the incident was mitigated before impacting BI's public services, as first reported by Reuters.

"BI is aware of a ransomware hack last month. We are aware that we have been hit by a cyber attack. This is a crime, it is real, and we are exposed to it," the head of BI's communications department, Erwin Haryono, told local media.

Conti claims the attack, leaks data

While Bank Indonesia did not attribute the attack to a specific ransomware gang, Conti has claimed the attack today after leaking some files allegedly stolen from Bank Indonesia's network.

In all, the ransomware group claims to have 13.88 GB worth of documents to leak if Bank Indonesia doesn't pay the ransom.

A Bank Indonesia spokesperson was not available for comment when contacted by BleepingComputer earlier today.

Image: BleepingComputer

The Conti ransomware gang

Conti is a Ransomware-as-a-Service (RaaS) operation linked to the Wizard Spider Russian cybercrime group, also known for other notorious malware, including Ryuk, TrickBot, and BazarLoader.

The ransomware group's affiliates breach targets' networks after corporate devices get infected with BazarLoader or TrickBot malware, providing them remote access to the compromised system.

After gaining access to the victim's internal network, the Conti operators will compromise other devices spreading through the victim's network.

This allows them to harvest and exfiltrate data before deploying the ransomware payloads across the network.

Conti is known for attacking high-profile organizations, including Ireland's Department of Health (DoH) and Health Service Executive (HSE), and marketing giant RR Donnelly (RRD).

Due to increased Conti activity, the FBI, CISA, and the NSA US have also recently issued an advisory warning of an increased number of Conti ransomware attacks.

Source: https://www.bleepingcomputer.com/news/security/indonesias-central-bank-confirms-ransomware-attack-conti-leaks-data/