Indonesia won't pay an $8 million ransom after a cyberattack compromised the national data center

June 24 2024, by Niniek Karmini

Officers check the passports of passengers leaving for Singapore at the immigration checkpoint of the Bandar Bentan Telani ferry terminal on Bintan Island, Indonesia, Wednesday, May 15, 2024. Indonesian authorities said Monday that the country's national data center was compromised by a cyber attack, disrupting public services including the immigration check points and asked for an $8 million ransom. Credit: AP Photo/Dita Alangkara, File

Indonesia's national data center has been compromised by a hacking group asking for a $8 million ransom that the government says it won't pay.

The cyberattack has disrupted services of more than 200 government agencies at both the national and regional levels since last Thursday, said Samuel Abrijani Pangerapan, the director general of informatics applications with the Communications and Informatics Ministry.

Some government services have returned—immigration services at airports and elsewhere are now functional—but efforts continue at restoring other services such as investment licensing, Pangerapan told reporters Monday.

The attackers have held data hostage and offered a key for access in return for the $8 million ransom, said PT Telkom Indonesia's director of network & IT solutions, Herlan Wijanarko, without giving further details.

Wijanarko said the company, in collaboration with authorities at home and abroad, is investigating and trying to break the encryption that made data inaccessible.

Communication and Informatics Minister Budi Arie Setiadi told journalists that the government won't pay the ransom.

"We have tried our best to carry out recovery while the (National Cyber and Crypto Agency) is currently carrying out forensics," Setiadi added.

The head of that agency, Hinsa Siburian, said they had detected samples of the Lockbit 3.0 ransomware.

Pratama Persadha, Indonesia's Cybersecurity Research Institute chairman, said the current cyberattack was the most severe in a series of ransomware attacks that have hit Indonesian government agencies and companies since 2017.

"The disruption to the national data center and days-long needed to recover the system means this ransomware attack was extraordinary," Persadha said. "It shows that our cyber infrastructure and its server systems were not being handled well."

He said a ransomware attack would be meaningless if the government had a good backup that could automatically take over the main server of the national data center during a cyberattack.

Indonesia's central bank was attacked by ransomware in 2022 but public services were not affected. The health ministry's COVID-19 app was hacked in 2021, exposing the personal data and health status of 1.3 million people.

Last year, an intelligence platform that monitors malicious activities in cyberspace, Dark Tracer, revealed that a hacker group known as the LockBit ransomware had claimed to have stolen 1.5 terabytes of data managed by Indonesia's largest Islamic bank, Bank Syariah Indonesia.