Australia blames Russian hackers for medical data theft

November 11 2022, by Steven TRASK

Hackers are demanding US$10 million to stop leaking sensitive records they stole from Medibank, Australia's largest private health insurer.

Russian hackers carried out a cyberattack on a major Australian healthcare company that breached the data of 9.7 million people, including the country's prime minister, police said Friday.

The hackers started leaking the data this week after Medibank, the country's largest health insurer, refused to pay a $9.7 million (Aus$15 million) ransom.

Australian Federal Police commissioner Reece Kershaw blamed the attack on Russia-based "cyber criminals".

"We believe those responsible for the breach are in Russia," he told reporters.

"Our intelligence points to a group of loosely affiliated cyber criminals who are likely responsible for past significant breaches across the world."

The hackers have been drip-feeding the stolen data to a dark web forum.

The first leaks appeared to have been selected to cause maximum harm: targeting those who received treatment related to drug abuse, sexually transmitted infections, or pregnancy terminations.

Kershaw said the hackers also appeared to be supported by people living outside Russia.

"These cyber criminals are operating like a business with affiliates and associates who are supporting the business.

"We also believe that some affiliates may be in other countries."

He added that Australian police would be working with Interpol and seeking the cooperation of their counterparts in Russia.

"We'll be holding talks with Russian law enforcement about these individuals," he said.

"Russia benefits from the intelligence sharing and data shared through Interpol and with that comes responsibilities and accountability."

Retaliation threat

Australia has repeatedly condemned Russia's invasion of Ukraine and has provided Kyiv with hundreds of millions of dollars in aid and military equipment.

Australia's foreign intelligence agency in April warned that backing Ukraine could open the country up to reprisals from Russian hackers.

"Russian-aligned cybercrime groups have threatened to conduct cyber operations in retaliation for perceived cyber offensives against the Russian government," the Australian Signals Directorate said in an advisory note.

"Some groups have also threatened to conduct cyber operations against countries and organisations providing materiel support to Ukraine."

Kershaw said police knew the identities of the hackers but he would not be naming them.

Cybersecurity analysts have suggested they could be linked to Russian hacker group REvil.

REvil—an amalgam of ransomware and evil—was reportedly dismantled by Russian authorities earlier this year, after extracting an $11 million ransom from JBS Foods, a major food conglomerate.

'Rolled gold mongrels'

Australian National University cybersecurity expert Thomas Haines said tracking the hackers down was the easiest part for police.

"It's unusual for hackers to cover their tracks so well that you don't know where they came from," he told AFP.

"But there are certain areas of the world where the ability to apply any pressure is effectively zero."

Kershaw said Australian police were taking "covert measures" to bring the hackers to justice.

"To the criminals, you know we know who you are," he said.

"The Australian Federal Police has some significant runs on the scoreboard when it comes to bringing overseas offenders back to Australia to face the justice system."

Education Minister Jason Clare on Friday called the hackers "rolled gold mongrels", while Home Affairs Minister Clare O'Neil has dubbed them "scummy criminals".

O'Neil on Thursday said the "smartest and toughest" people in Australia were hunting down the hackers.

In a taunting reply posted to the dark web early Friday morning, the hackers said: "We always keep our word."

"We should post this data, because nobody will believe us in the future."

Citation: Australia blames Russian hackers for medical data theft (2022, November 11) retrieved