The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Australia Blames Russian Hacker for Major Cyber Attack

By AFP

January 23, 2024

Russian hacker Aleksandr Ermakov. **DFAT**

Australia has identified the Russian mastermind behind a crippling cyber attack, unmasking the 33-year-old hacker for the first time on Tuesday and linking him to an international crime syndicate.

Hackers infiltrated Australian private health insurer Medibank in November 2022, stealing sensitive medical records and leaking them on the dark web.

Among the 9.7 million customers caught up in the high-profile cyber attack — one of the country's worst data breaches — was Australian Prime Minister Anthony Albanese.

Australian intelligence agencies have long suspected Russian hackers were behind the breach, which had previously been tentatively linked to the REvil ransomware collective.

Following an 18-month investigation, Australia has now taken the rare step of naming the

individual believed responsible — Russian citizen Aleksandr Gennadievich Ermakov, who has also been hit with first-of-their-kind cyber sanctions.

"This is the first time an Australian government has identified a cyber criminal and imposed cyber sanctions of this kind and it won't be the last," Home Affairs Minister Clare O'Neil told reporters.

"These people are cowards and they're scumbags," she added.

"They hide behind technology, and today the Australian government is saying that when we put our minds to it, we'll unveil who you are, and we'll make sure you are accountable."

The Medibank hackers started leaking private health records on the dark web after the company, one of Australia's largest private health insurers, refused to pay a multi-million dollar ransom.

The leaks were selected to cause maximum harm, targeting records related to drug abuse, sexually transmitted infections and pregnancy terminations.

"Medibank, in my view, was the single most devastating cyber attack we have experienced as a nation," O'Neil said Tuesday.

"We all went through it, literally millions of people having personal data about themselves, their family members, taken from them and cruelly placed online for others to see."

'Hack the hackers'

Australia beefed up its cyber security laws in the wake of the Medibank attack, pledging that the country's intelligence agencies would proactively "hack the hackers."

In a taunting and cryptic reply posted to the dark web, the hackers responded: "We always keep our word."

Ermakov, who used the online aliases blade_runner and JimJones, would now be targeted by a travel ban and strict financial sanctions, Foreign Minister Penny Wong said.

"This will mean it's a criminal offense, punishable with up to 10 years imprisonment, to provide assets to him — or to use or deal with his assets," she told reporters.

Photos released by the Australian government showed Ermakov as a fresh-faced young man with short dark hair.

REvil — an amalgam of ransomware and evil — was reportedly dismantled by Russian authorities in 2022 after it extorted an $11 million ransom from JBS Foods, a major food conglomerate.

The Australian government confirmed Ermakov was a member of the REvil syndicate.

Monash University cyber crime expert Nigel Phair said proving who was behind an attack was "one of the hardest things to do" in cyber security.

"This is unlikely to dissuade other internationally-based cyber criminals from targeting Australian organizations or individuals, but is a step in the right direction," he said.

Defence Minister Richard Marles said Australia's intelligence agencies had tracked down Ermakov with the help of the National Security Agency in the United States, and GCHQ in the United Kingdom.

"Ermakov doesn't have anonymity," he said.

"We have named him for the first time globally. And his identity is now on display for every agency around the world."