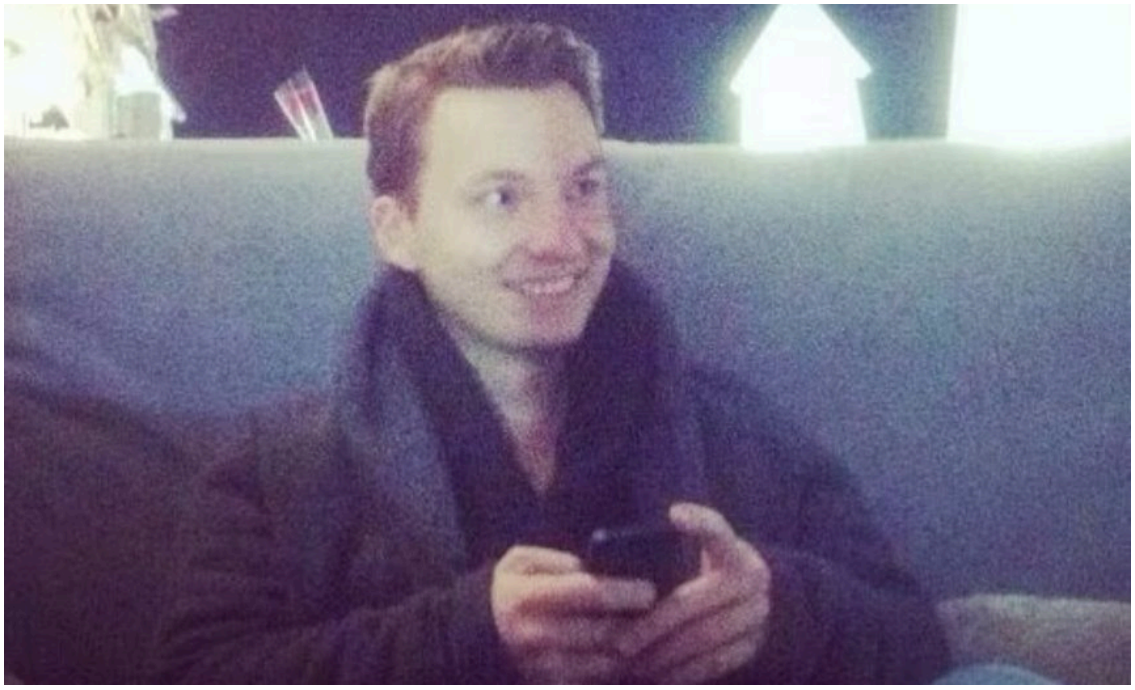
Australia, US, UK Sanction Russian Over 2022 Medibank Breach

By Mihir Bagwe

Archived: 2026-04-05 14:05:56 UTC

Fraud Management & Cybercrime , Geo-Specific , Ransomware

Governments Accuse Aleksandr Ermakov and REvil of Being Medibank Hackers (MihirBagwe) • January 23, 2024



The United States, the United Kingdom and Australia accused Aleksandr Ermakov, pictured, of hacking Medibank in 2022. (Image: Australian Department of Foreign Affairs and Trade)

The United States, Australia and the United Kingdom sanctioned a Russian man the governments say was behind the October 2022 hacking of Medibank, Australia's largest private health insurer.

See Also: Demostración Del Producto: Backup Y Recuperación De VM

Australia on Monday sanctioned 33-year-old Aleksandr Gennadievich Ermakov, linking him to the Medibank data breach - an incident that resulted in hackers dumping online information taken from 9.7 million current and former Medibank customers (see: *Medibank Hackers Dump Stolen Data on the Dark Web*).

The United States and the United Kingdom followed suit Tuesday. The coordinated trilateral action, a first for the countries, "underscores our collective resolve to hold these criminals to account," said U.S. Under Secretary of the Treasury Brian Nelson.

Australian authorities announced in November 2022 that they had identified the Medibank hackers, citing "a group of loosely affiliated cybercriminals" based in Russia. The hackers may be a relaunch of the REvil extortion gang known as BlogXX (see: *Who Is Extorting Australian Health Insurer Medibank?*). The U.S. Treasury announcement says that Ermakov and the other actors behind the Medibank hack "are believed to be linked to the Russia-backed cybercrime gang REvil."

Australian Foreign Affairs Minister Penny Wong signed the sanctions decision against Ermakov on Monday. His various aliases include AlexanderErmakov, GustaveDore, aiiis_ermak, blade_runner and JimJones.

The attack was a high point in a wave of ransomware attacks and data breaches buffeting the country that year. It ended with the government vowing to wake "from a cyber slumber" and become " "the world's most cyber-secure country" over the next seven years (see: Australia Aims to Be World's 'Most Cyber-Secure' Country).

Medibank refused to pay hackers' extortion demand, stating at the time that it believed the chances of limiting the breach fallout were "limited" and that "there is a strong chance that paying puts more people in harm's way by making Australia a bigger target."

"Today is a warning to cybercriminals," said Australian Minister for Cyber Security Clare O'Neil while announcing the sanctions. "We will never stop looking for you. We will unveil who you are, and we will make sure you are held accountable."

The Australian sanctions ban Ermakov from entering the country and make having financial dealings with him punishable by up to a decade in prison. The U.S. and U.K. sanctions ensure Ermakov's banishment from vast segments of the international financial system.
