The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Russia's 'Evil Corp' Hackers Unmasked by Sweeping Sanctions

By AFP

October 02, 2024

Lucas Andrade / pexels

A tight-knit family of hackers and intelligence operatives was the driving force behind Russia's "Evil Corp" cybercrime syndicate, sanctions leveled by London, Washington and Canberra have revealed.

Once considered the "most significant cybercrime threat in the world," Evil Corp has been credited with spying on NATO allies at the behest of Russia's intelligence services.

It has also used phishing scams to pilfer more than $100 million from a string of companies across dozens of countries, according to a 2019 US indictment.

Financial sanctions rolled out by the United Kingdom, the United States and Australia jointly target Evil Corp figures such as Maksim Yakubets, the leader of the hacking group.

But the sanctions also shed light on the tight-knit nature of the group's operations, detailing

a family tree that included Yakubets' brother, cousins and father.

On Tuesday, the U.S. Treasury also sanctioned Eduard Benderskiy — a former Spetsnaz officer and Yakubets' father-in-law — who was suspected of orchestrating "Evil Corp's relationship with the Russian state."

Related article: Germany Accuses Russia's GRU Military Intelligence of Cyberattacks on NATO, EU

"Today's sanctions send a clear message to the Kremlin that we will not tolerate Russian cyber-attacks — whether from the state itself or from its cyber-criminal ecosystem," UK Foreign Secretary David Lammy said.

Australian Foreign Minister Penny Wong added: "We are using all elements of our national power to make Australia more secure and to keep Australians safe."

Additionally, all three nations leveled sanctions against Aleksandr Ryzhenkov, a previously unknown hacker who the UK's National Crime Agency linked to the prolific LockBit ransomware group.

LockBit was one of the major developers of malicious software that allows criminals to lock victims out of their networks, steal their data and demand a ransom for its return. In 2023, Canada's Communications Security Establishment estimated that LockBit was used in 44% of ransomware incidents worldwide.

Original url:
https://www.themoscowtimes.com/2024/10/02/russias-evil-corp-hackers-unmasked-by-sweeping-sanctions-a86542