United States, Australia, and the United Kingdom Sanction Russian Cyber Actor Responsible for the Medibank Hack

January 23, 2024

WASHINGTON — Today, the Department of the Treasury's Office of Foreign Assets Control (OFAC), in coordination with Australia and the United Kingdom, designated Alexander Ermakov (Ermakov), a cyber actor who played a pivotal in the 2022 ransomware attack against Medibank Private Limited, an Australian healthcare insurer.

"Russian cyber actors continue to wage disruptive ransomware attacks against the United States and allied countries, targeting our businesses, including critical infrastructure, to steal sensitive data," said Under Secretary of the Treasury Brian E. Nelson. "Today's trilateral action with Australia and the United Kingdom, the first such coordinated action, underscores our collective resolve to hold these criminals to account."

Yesterday, Australia sanctioned Ermakov for utilizing ransomware to attack the Medibank network and for the exfiltration of sensitive data of 9.7 million users of Medibank services. Today, the United States and the United Kingdom, in solidarity with Australia, are taking action against the same individual because of the similar risk presented by this actor to the United States and the UK.

This action demonstrates that the United States stands with our partners to disrupt ransomware actors who victimize the backbone of our economies and critical infrastructure. Ransomware attacks against healthcare firms, which are frequent targets of ransomware attacks in the United States, present risks to patient care, safety, and sensitive personally identifiable data. Russia continues to provide a safe haven to ransomware actors like Ermakov, enabling cyber actors to freely perpetrate ransomware attacks and other malicious cyber activities from Russia. In addition, Russia has also enabled ransomware attacks by cultivating and co-opting criminal hackers. Treasury has previously stressed that Russia must take concrete steps to prevent cyber criminals from freely operating in its jurisdiction.

REVIL RANSOMWARE AND THE MEDIBANK HACK

In October 2022, Ermakov infiltrated the Medibank network, one of Australia's largest private health insurers, covering over 3.9 million people with over 4,000 employees. During the attack, Ermakov stole Personally Identifiable Information (PII) and sensitive health information linked to approximately 9.7 million current and former customers and authorized representatives. Ermakov and the other actors behind the Medibank hack are believed to be linked to the Russia-backed cybercrime gang REvil.

REvil was among the most notorious cybercrime gangs in the world until July 2021 when they disappeared. REvil is a ransomware-as-a-service (RaaS) operation and generally motivated by financial gain. REvil ransomware has been deployed on approximately 175,000 computers worldwide, with at least $200 million paid in ransom. Today's action follows previous Treasury designations of two individuals for perpetuating Sodinokibi/REvil ransomware incidents against the United States.

RANSOMWARE ACTORS BEHIND MEDIBANK HACK

Ermakov is a Russian national and cybercriminal. He has been sanctioned for his role in the exfiltration and release on the dark net of 9.7 million records containing the personal information of Australians, including names, dates of birth, Medicare numbers, and sensitive medical information.

OFAC is designating Ermakov pursuant to Executive Order (E.O.) 13694, as amended by E.O. 13757, for being responsible for or complicit in, or to have engaged in, directly or indirectly, an activity described in subsection (a)(ii) of section 1 of E.O. 13694, as amended.

SANCTIONS IMPLICATIONS

As a result of today's action, all property and interests in property of the individual described above that are in the United States or in the possession or control of U.S. persons must be blocked and reported to OFAC. OFAC's regulations generally prohibit all dealings by U.S. persons or within the United States (including transactions transiting the United States) that involve any property or interests in property of a blocked or designated person. In addition, any entities that are owned, directly or indirectly, 50 percent or more by one or more blocked persons are also blocked. All transactions by U.S. persons or within (or transiting) the United States that involve any property or interests in property of designated or blocked persons are prohibited unless authorized by a general or specific license issued by OFAC, or exempt. These prohibitions include the making of any contribution or provision of funds, goods, or services

by, to, or for the benefit of any blocked person and the receipt of any contribution or provision of funds, goods, or services from any such person.

In addition, persons that engage in certain transactions with the individual designated today may themselves be exposed to sanctions.

The power and integrity of sanctions derive not only from OFAC's ability to designate and add persons to the Specially Designated Nationals and Blocked Persons (SDN) List but also from its willingness to remove persons from the SDN List consistent with the law. The ultimate goal of sanctions is not to punish but to bring about a positive change in behavior. For information concerning the process for seeking removal from an OFAC list, including the SDN List, please refer to OFAC's Frequently Asked Question 897 here. For detailed information on the process to submit a request for removal from an OFAC sanctions list, please click here.

For identifying information on the individuals designated today, click here.

To report a cyber-crime, contact the Federal Bureau of Investigation's Internet Crime Complaint Center.

###