

United States Sanctions Affiliates of Russia-Based LockBit Ransomware Group

February 20, 2024

The United States imposes sanctions on affiliates of group responsible for ransomware attacks on the U.S. financial sector

WASHINGTON — Today, the United States is designating two individuals who are affiliates of the Russia-based ransomware group LockBit. This action is the first in an ongoing collaborative effort with the U.S. Department of Justice, Federal Bureau of Investigation, and our international partners targeting LockBit.

“The United States will not tolerate attempts to extort and steal from our citizens and institutions,” said Deputy Secretary of the Treasury Wally Adeyemo. “We will continue our whole-of-government approach to defend against malicious cyber activities, and will use all available tools to hold the actors that enable these threats accountable.”

Russia continues to offer safe harbor for cybercriminals where groups such as LockBit are free to launch ransomware attacks against the United States, its allies, and partners. These ransomware attacks have targeted critical infrastructure, including hospitals, schools, and financial institutions. Notably, LockBit was responsible for the November 2023 ransomware attack against the Industrial and Commercial Bank of China’s (ICBC) U.S. broker-dealer. The United States is a global leader in the fight against cybercrime and is committed to using all available authorities and tools to defend Americans from cyber threats. In addition to the actions announced today, the U.S. government provides critical resources to support potential victims in protecting against and responding to ransomware attacks. For example, last year, the Cybersecurity & Infrastructure Security Agency in conjunction with other U.S. Departments and Agencies and foreign partners published two cybersecurity advisories, “[Understanding Ransomware Threat Actors: LockBit](#)” and “[LockBit 3.0 Ransomware Affiliates Exploit CVE 2023-4966 Citrix Bleed Vulnerability](#).” These advisories detail the threats posed by this group and provide recommendations to reduce the likelihood and impact of future ransomware incidents.

This action follows other recent actions taken by the U.S. against Russian cybercriminals, including the recent trilateral designation of Alexander Ermakov, a Russian national involved in the 2022 ransomware attack against Medibank Private Limited, in coordination with Australia and the United Kingdom and last year's bilateral [sanctions actions](#) against the Trickbot Cybercrime Group with the United Kingdom. Russia has 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. Today's actions reflect the United States' commitment to combatting cybercrime and pursuing the bad actors that target victims across the United States, its allies, and its partners.

LOCKBIT: A MALICIOUS RUSSIAN RANSOMWARE GROUP

LockBit is a Russia-based ransomware group first observed in 2019 and best known for its ransomware variant of the same name. LockBit operates on a Ransomware-as-a-Service (RaaS) model, where the group licenses its ransomware software to affiliated cybercriminals in exchange for a percentage of the paid ransoms. LockBit is known for its double extortion tactics, where its cybercriminals exfiltrate vast amounts of data from its victims before encrypting the victim's computer systems and demanding ransom payments. LockBit was the most deployed ransomware variant globally in 2022 and remains prolific today.

OFAC's investigation identified LockBit as responsible for the ransomware attack on ICBC, which occurred on November 9, 2023. The ransomware attack disrupted ICBC's U.S. broker-dealer, affecting the settlement of over \$9 billion worth of assets backed by Treasury securities. The ransomware attack caused a blackout of ICBC's computer systems, resulting in a loss of e-mail and communications. ICBC's inability to access its systems caused securities to be delivered for settlement with no funds backing the trades.

OFAC TARGETS AFFILIATES OF LOCKBIT RANSOMWARE GROUP

Ivan Gennadievich Kondratiev, a Russian national located in Novomokovsk, Russia, is a LockBit affiliate and leader of the LockBit affiliate sub-group, the National Hazard Society. Kondratiev is commonly known in the cybercriminal world as "Bassterlord" and "Fisheye," and he also has ties to REvil, RansomEXX and Avaddon ransomware groups. Kondratiev has actively engaged in LockBit ransomware attacks.



Artur Sungatov, a Russian national, is a Lockbit ransomware group affiliate and has actively engaged in LockBit ransomware attacks.

OFAC is designating each of these individuals pursuant to Executive Order (E.O.) 13694, as amended by E.O. 13757, for being responsible for or complicit in, or having engaged in, directly or indirectly, an activity described in subsection (a)(ii)(D) 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 designated persons described above that are in the United States or in the possession or control of U.S. persons are blocked and must be reported to OFAC. In addition, any entities that are owned, directly or indirectly, individually or in the aggregate, 50 percent or more by one or more blocked persons are also blocked. Unless authorized by a general or specific license issued by OFAC, or exempt, OFAC's regulations generally prohibit all transactions by U.S. persons or within (or transiting) the United States that involve any property or interests in property of designated or otherwise blocked persons. In addition, persons that engage in certain transactions with the individuals designated today may themselves be exposed to designation.

The power and integrity of OFAC sanctions derive not only from its 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](#).

See [OFAC's Updated Advisory on Potential Sanctions Risk for Facilitating Ransomware Payments](#)  for information on the actions that OFAC would consider to be mitigating factors in any related enforcement action involving ransomware payments with a potential sanctions risk. For information on complying with sanctions applicable to virtual currency, see [OFAC's Sanctions Compliance Guidance for the Virtual Currency Industry](#) .

[For more information on the individuals designated today, click here.](#)

###

