United States Sanctions Senior Leader of the LockBit Ransomware Group

May 7, 2024

The United States uncovers identity and imposes sanctions on Dmitry Khoroshev, a senior leader of the LockBit Ransomware group

WASHINGTON — Today, the United States designated Dmitry Yuryevich Khoroshev, a Russian national and a leader of the Russia-based LockBit group, for his role in developing and distributing LockBit ransomware. This designation is the result of a collaborative effort with the U.S. Department of Justice, Federal Bureau of Investigation, the UK's National Crime Agency and other international partners. Today, the Department of Justice is unsealing an indictment and the United Kingdom and Australia are also announcing the designation of Khoroshev.

"Today's action sends a clear message that the United States and its partners around the world are committed to dismantling the ransomware ecosystem, including by uncovering the identities of those perpetrating ransomware attacks against the United States," said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson. "We will persist in efforts to expose and hold accountable individuals responsible for deploying ransomware that threatens the security and safety of Americans and to seek justice for victims."

This designation follows several other recent U.S. actions against Russian cybercriminals, including the disruption of the LockBit ransomware infrastructure and sanctions against LockBit group affiliates. 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. 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 commitment of the United States to a long-term, coordinated, and sustained approach to disrupting and degrading the ransomware ecosystem.

Additionally, the U.S. Department of State (State) announced a reward of up to $10 million for information that leads to the identification or location of any individual(s) who hold a key

leadership position in the LockBit group. State is also offering a reward of $5 million for information leading to the arrest and/or conviction in any country of any individual conspiring to participate in or attempting to participate in LockBit ransomware activities.

LOCKBIT: ONE OF THE MOST PROLIFIC RANSOMWARE GROUP IN THE WORLD

The Russia-based LockBit ransomware group is one of the most active ransomware groups in the world and is best known for its ransomware variant of the same name. It has targeted over 2,500 victims worldwide and is alleged to have received more than $500 million in ransom payments. Since January 2020, affiliates using LockBit have attacked organizations across an array of critical infrastructure sectors, including financial services, food and agriculture, education, emergency services, and healthcare.

LockBit operates on a Ransomware-as-a-Service model, where the group licenses its ransomware software to affiliated cybercriminals in exchange for a percentage of the paid ransoms. A Ransomware-as-a-Service cybercrime group maintains the functionality of a particular ransomware variant, sells access to that ransomware variant to individuals or groups of operators (often referred to as “affiliates”), and supports affiliates’ deployment of their ransomware in exchange for upfront payment, subscription fees, a cut of profits, or a combination of upfront payment, subscription fees, and a cut of profits. Additionally, 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.

On November 9, 2023, LockBit conducted the ransomware attack on the Industrial and Commercial Bank of China (ICBC)’s U.S. broker-dealer. The group is also responsible for the December 18, 2023 ransomware attack that targeted Chicago’s Saint Anthony Hospital, in which LockBit demanded a ransom payment from the hospital to stop the release of patient files on the dark web.

CYBERCRIMINAL RESPONSIBLE FOR THE LOCKBIT RANSOMWARE VARIANT EXPOSED

Dmitry Yuryevich Khoroshev (**Khoroshev**), a Russian national and a leader of LockBit, is the primary operator of the well-known and public-facing LockBit-related cybercrime moniker, “LockBitSupp.” As a core LockBit group leader and developer of the LockBit ransomware,

Khoroshev has performed a variety of operational and administrative roles for the cybercrime group, and has benefited financially from the LockBit ransomware attacks. In addition, **Khoroshev** has facilitated the upgrading of the LockBit infrastructure, recruited new developers for the ransomware, and managed LockBit affiliates. He is also responsible for LockBit's efforts to continue operations after their disruption by the U.S. and its allies earlier this year.

OFAC is designating **Khoroshev** 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) 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 individuals 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 blocked or designated persons.

In addition, persons that engage in certain transactions with the individuals designated today may themselves be exposed to designation. Furthermore, any foreign financial institution that knowingly facilitates a significant transaction or provides significant financial services for any of the individuals or entities designated today could be subject to U.S. correspondent or payable-through account sanctions.

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 Risks 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 nexus. For information on complying with sanctions applicable to virtual currency, see OFAC's Sanctions Compliance Guidance for the Virtual Currency Industry.

Further, 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.

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

###