United States and United Kingdom Sanction Additional Members of the Russia-Based Trickbot Cybercrime Gang

Published: 2026-02-13 · Archived: 2026-04-05 16:33:11 UTC

U.S. Department of Justice Concurrently Unsealing Nine Indictments

WASHINGTON — Today, the United States, in coordination with the United Kingdom, sanctioned eleven individuals who are part of the Russia-based Trickbot cybercrime group. Russia has long been a safe haven for cybercriminals, including the Trickbot group. Today's action was taken by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC). The U.S. Department of Justice (DOJ) is concurrently unsealing indictments against nine individuals in connection with the Trickbot malware and Conti ransomware schemes, including seven of the individuals designated today.

Today's targets include key actors involved in management and procurement for the Trickbot group, which has ties to Russian intelligence services and has targeted the U.S. Government and U.S. companies, including hospitals. During the COVID-19 pandemic, the Trickbot group targeted many critical infrastructure and health care providers in the United States.

"The United States is resolute in our efforts to combat ransomware and respond to disruptions of our critical infrastructure," said Under Secretary of the Treasury Brian E. Nelson. "In close coordination with our British partners, the United States will continue to leverage our collective tools and authorities to target these malicious cyber activities."

The targets designated today include administrators, managers, developers, and coders who have materially assisted the Trickbot group in its operations. This designation is part of continued collaborative efforts by the U.S. and the UK to disrupt Russian cybercrime and ransomware, and follows the first joint U.S.-UK cyber designation of several Trickbot group members in February 2023, the first designation under the UK's new cyber authority. Treasury coordinated extensively with UK partners, including the Foreign, Commonwealth, and Development Office; National Crime Agency; and His Majesty's Treasury. Today's action represents the continued commitment of the United States and the United Kingdom to target, combat, and counter ransomware actors and to address Russian cybercrime.

TRICKBOT: RUSSIA'S NOTORIOUS CYBER GANG

Trickbot, first identified in 2016 by security researchers, was a trojan virus that evolved from the Dyre trojan. Dyre was an online banking trojan operated by Moscow-based individuals who began targeting non-Russian businesses and entities in mid-2014. Dyre and Trickbot were developed and operated by a group of cybercriminals to steal financial data from targets outside of Russia. The Trickbot trojan infected millions of victim computers worldwide, including those of U.S. businesses and individuals. It has since evolved into a highly modular malware suite that provides the Trickbot group the ability to conduct a variety of malicious cyber activities, including ransomware. During the height of the COVID-19 pandemic in 2020, the Trickbot group launched a wave of

ransomware disruptions against hospitals and other healthcare centers across the United States. In one instance, the Trickbot group deployed ransomware against three Minnesota medical facilities, disrupting their computer networks and telephones, and causing a diversion of ambulances. Members of the Trickbot group publicly gloated over the ease of targeting the medical facilities and the speed with which ransoms had been paid to the group. Members of the Trickbot group are associated with Russian intelligence services. The Trickbot group's preparations in 2020 aligned them to Russian state objectives and actions taken by the Russian intelligence services. This included targeting the U.S. Government and U.S. companies.

Andrey Zhuykov was a central actor in the group and acted as a senior administrator. Andrey Zhuykov is also known by the online monikers Dif and Defender.

Maksim Galochkin led a group of testers, with responsibilities for development, supervision, and implementation of tests. Maksim Galochkin is also known by the online monikers Bentley, Crypt, and Volhvb.

Maksim Rudenskiy was a key member of the Trickbot group and the team lead for coders.

Mikhail Tsarev was a manager with the group, overseeing human resources and finance. He was responsible for management and bookkeeping. Mikhail Tsarev is also known by the monikers Mango, Alexander Grachev, Super Misha, Ivanov Mixail, Misha Krutysha, and Nikita Andreevich Tsarev.

Dmitry Putilin was associated with the purchase of Trickbot infrastructure. Dmitry Putilin is also known by the online monikers Grad and Staff.

Maksim Khaliullin was an HR manager for the group. He was associated with the purchase of Trickbot infrastructure including procuring Virtual Private Servers. Maksim Khaliullin is also known by the online moniker Kagas.

Sergey Loguntsov was a developer for the Trickbot group.

Vadym Valiakhmetov worked as a coder for the Trickbot group and is known by the online monikers Weldon, Mentos, and Vasm.

Artem Kurov worked as a coder with development duties in the Trickbot group. Artem Kurov is also known by the online moniker Naned.

Mikhail Chernov was part of the internal utilities group for Trickbot and is also known by the online moniker Bullet.

Alexander Mozhaev was part of the admin team responsible for general administrative duties and is also known by the online monikers Green and Rocco.

OFAC is designating each of these individuals pursuant to Executive Order (E.O.) 13694, as amended by E.O. 13757, for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, 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. For detailed information on the process to submit a request for removal from an OFAC sanctions list, please refer to OFAC's website.

See OFAC's Updated Advisory on Potential Sanctions Risk for Facilitating Ransomware Payments here, 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 here. See also the UK's Office of Financial Sanctions Implementation's recently issued Guidance on Financial Sanctions and Ransomware.

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

###
