

U.S. DEPARTMENT OF THE TREASURY

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

February 9, 2023


The United States and United Kingdom issue historic joint cyber sanctions

WASHINGTON — Today, the United States, in coordination with the United Kingdom, is designating seven individuals who are part of the Russia-based cybercrime gang Trickbot. This action represents the very first sanctions of their kind for the U.K., and result from a collaborative partnership between the U.S. Department of the Treasury's Office of Foreign Assets Control and the U.K.'s Foreign, Commonwealth, and Development Office; National Crime Agency; and His Majesty's Treasury to disrupt Russian cybercrime and ransomware.

“Cyber criminals, particularly those based in Russia, seek to attack critical infrastructure, target U.S. businesses, and exploit the international financial system,” said Under Secretary Brian E. Nelson. “The United States is taking action today in partnership with the United Kingdom because international cooperation is key to addressing Russian cybercrime.”

Russia is a haven for cybercriminals, where groups such as Trickbot freely perpetrate malicious cyber activities against the U.S., the U.K., and allies and partners. These malicious cyber activities have targeted critical infrastructure, including hospitals and medical facilities during a global pandemic, in both the U.S. and the U.K. Last month, [Treasury's Financial Crimes Enforcement Network \(FinCEN\) identified a Russia-based virtual currency exchange, Bitzlato Limited](#), as a “primary money laundering concern” in connection with Russian illicit finance.

The United States and the United Kingdom are leaders in the global fight against cybercrime and are committed to using all available authorities and tools to defend against cyber threats.

This action follows other recent sanctions actions taken jointly by the U.S. and the U.K. including in the Russia and Burma programs, as well as last year's [multilateral action against the Kinahan Crime Group](#). It also reflects the finding from the [2021 Sanctions Review](#)  that sanctions are most effective when coordinated with international partners and highlights the [deepened partnership between OFAC and the UK's Office of Financial Sanctions Implementation](#).

TRICKBOT: A NOTORIOUS CYBER GANG IN RUSSIA

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 individuals based in Moscow, Russia, that 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. The Trickbot trojan viruses infected millions of victim computers worldwide, including those of U.S. businesses, and individual victims. It has since evolved into a highly modular malware suite that provides the Trickbot Group with the ability to conduct a variety of illegal cyber activities, including ransomware attacks. During the height of the COVID-19 pandemic in 2020, Trickbot targeted hospitals and healthcare centers, launching a wave of ransomware attacks against hospitals across the United States. In one of these attacks, 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 the ransoms were paid to the group.

Current 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 targeting previously conducted by Russian Intelligence Services. This included targeting the U.S. government and U.S. companies.

Vitaly Kovalev was a senior figure within the Trickbot Group. Vitaly Kovalev is also known as the online monikers "Bentley" and "Ben". Today, an indictment was unsealed in the U.S. District Court for the District of New Jersey charging Kovalev with conspiracy to commit bank fraud and eight counts of bank fraud in connection with a series of intrusions into victim bank accounts held at various U.S.-based financial institutions that occurred in 2009 and 2010, predating his involvement in Dyre or the Trickbot Group.

Maksim Mikhailov has been involved in development activity for the Trickbot Group. Maksim Mikhailov is also known as the online moniker "Baget".

Valentin Karyagin has been involved in the development of ransomware and other malware projects. Valentin Karyagin is also known as the online moniker "Globus".

Mikhail Iskritskiy has worked on money-laundering and fraud projects for the Trickbot Group. Mikhail Iskritskiy is also known as the online moniker "Tropa".

Dmitry Pleshevskiy worked on injecting malicious code into websites to steal victims' credentials. Dmitry Pleshevskiy is also known as the online moniker "Iseldor".

Ivan Vakhromeyev has worked for the Trickbot Group as a manager. Ivan Vakhromeyev is also known as the online moniker "Mushroom".

Valery Sedletski has worked as an administrator for the Trickbot Group, including managing servers. Valery Sedletski is also known as the online moniker "Strix".


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 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](#)  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](#) . 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.](#)

[For more information on the United Kingdom's action, click here.](#)

###