Treasury Sanctions Members of the Russia-Based Cybercriminal Group Evil Corp in Tri-Lateral Action with the United Kingdom and Australia

Published: 2026-02-13 · Archived: 2026-04-06 03:20:37 UTC

The United States takes additional action against the Russia-based cybercriminal group Evil Corp, identifying and sanctioning additional members and affiliates

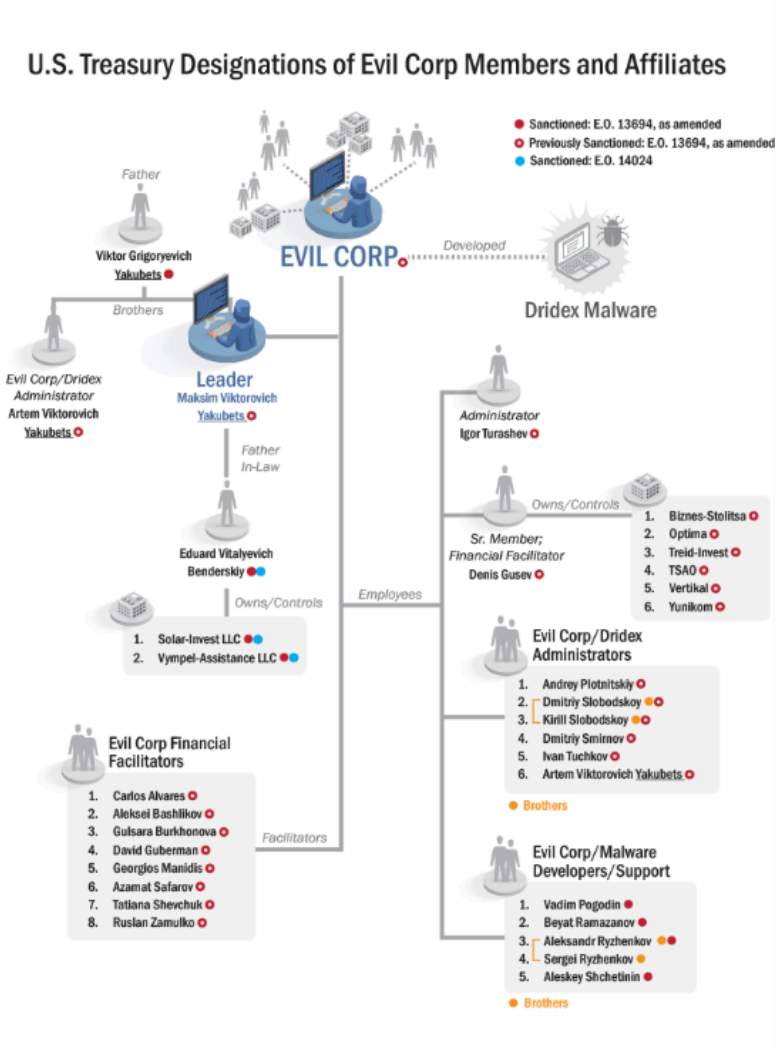
WASHINGTON — Today, the Department of the Treasury's Office of Foreign Assets Control (OFAC) is designating seven individuals and two entities associated with the Russia-based cybercriminal group Evil Corp, in a tri-lateral action with the United Kingdom's Foreign, Commonwealth & Development Office (FCDO) and Australia's Department of Foreign Affairs and Trade (DFAT). On December 5, 2019, OFAC designated Evil Corp, its leader and founder Maksim Viktorovich Yakubets and over a dozen Evil Corp members, facilitators, and affiliated companies pursuant to Executive Order (E.O.) 13694, as amended by E.O. 13757 ("E.O. 13694, as amended"). The United Kingdom and Australia are concurrently designating select Evil Corp-affiliated individuals designated by OFAC today or in 2019. Additionally, the U.S. Department of Justice has unsealed an indictment charging one Evil Corp member in connection with his use of BitPaymer ransomware targeting victims in the United States. Today's designation also coincides with the second day of the U.S.-hosted Counter Ransomware Initiative summit which involves over 50 countries working together to counter the threat of ransomware.

"Today's trilateral action underscores our collective commitment to safeguard against cybercriminals like ransomware actors, who seek to undermine our critical infrastructure and threaten our citizens," said Acting Under Secretary of the Treasury for Terrorism and Financial Intelligence Bradley T. Smith. "The United States, in close coordination with our allies and partners, including through the Counter Ransomware Initiative, will continue to expose and disrupt the criminal networks that seek personal profit from the pain and suffering of their victims."

Evil Corp is a Russia-based cybercriminal organization responsible for the development and distribution of the Dridex malware. Evil Corp has used the Dridex malware to infect computers and harvest login credentials from hundreds of banks and other financial institutions in over 40 countries, resulting in more than $100 million in theft losses and damage suffered by U.S. and international financial institutions and their customers. In a concurrent action with OFAC's December 2019 sanctions designations, the U.S. Department of Justice indicted Maksim and Evil Corp administrator Igor Turashev on criminal charges related to computer hacking and bank fraud schemes, and the U.S. Department of State's Transnational Organized Crime Rewards Program issued a reward for information of up to $5 million leading to the capture and/or conviction of Maksim.

Additionally, Maksim used his employment at the Russian National Engineering Corporation (NIK) as cover for his ongoing criminal activities linked to Evil Corp. The NIK was established by Igor Yuryevich Chayka (Chayka), son of Russian Security Council member Yuriy Chayka, and his associate Aleksei Valeryavich Troshin (Troshin). In October 2022, OFAC designated Chayka, Troshin, and NIK pursuant to E.O. 14024.

Evil Corp Members and Affiliates



Click-to-Enlarge

Eduard Benderskiy (Benderskiy), a former Spetnaz officer of the Russian Federal Security Service (FSB), which is designated under numerous OFAC sanctions authorities, current Russian businessman, and the father-in-law of Evil Corp's leader Maksim Viktorovich Yakubets (Maksim), has been a key enabler of Evil Corp's relationship with the Russian state. Benderskiy leveraged his status and contacts to facilitate Evil Corp's developing relationships with officials of the Russian intelligence services. After the December 2019 sanctions and indictments against Evil Corp and Maksim, Benderskiy used his extensive influence to protect the group.

While he has no official position in the Russian government, Benderskiy portrays himself as an aide to the Russian Duma. Around 2017, one of Benderskiy's private security firms was involved in providing security for Iraq-based facilities operated by the Russian oil company Lukoil OAO. This same private security firm has been lauded by the FSB, the Russian Ministry of Foreign Affairs, the Russian Duma, and other Russian government bodies.

From at least 2016, Maksim had business interactions with Aleksandr Tikhonov (Tikhonov), former commander of the FSB Special purpose Center, Russian government leaders, including OFAC-designated persons Dmitry

Kozak (Kozak) and Gleb Khor, and leaders of prominent Russian banks like OFAC-designated person Herman Gref (Gref), the Chief Executive Officer of Sberbank. In 2019, Benderskiy used his connections to facilitate a business deal that included Maksim and Kozak, which they believed would earn tens of millions of dollars per month. In the same year, Benderskiy hosted a meeting with Maksim and Gref to discuss business contracts with NIK.

After the December 2019 sanctions and indictments against Evil Corp and Maksim, Maksim sought out Benderskiy's guidance. Benderskiy used his extensive influence to protect the group, including his son-in-law, both by providing senior members with security and by ensuring they were not pursued by Russian internal authorities.

OFAC designated Benderskiy pursuant to E.O. 14024 for being owned or controlled, or having acted or purported to act for or on behalf of, directly or indirectly, the Government of the Russian Federation, and pursuant to E.O. 13694, as amended, for having materially assisted, sponsored, or provided financial, material, or technological support, or goods or services in support of, Maksim, a person whose property and interests in property are blocked pursuant to E.O. 13694, as amended.

Benderskiy is the general director, founder, and 100 percent owner of the Russia-based business and management consulting companies **Vympel-Assistance LLC** and **Solar-Invest LLC**. OFAC designated Vympel-Assistance LLC and Solar-Invest LLC pursuant to E.O. 14024 and E.O. 13694, as amended, for being owned or controlled, or having acted or purported to act for or on behalf of, directly or indirectly, Benderskiy, a person whose property and interests in property are blocked pursuant to E.O. 14024 and E.O. 13694, as amended.

Viktor Grigoryevich Yakubets (Viktor) is Maksim's father and a member of Evil Corp. In 2020, Viktor likely procured technical equipment in furtherance of Evil Corp's operations. OFAC designated Viktor pursuant to E.O. 13694, as amended, for having materially assisted, sponsored, or provided financial, material, or technological support, or goods or services in support of, Evil Corp, a person whose property and interests in property are blocked pursuant to E.O. 13694, as amended.

Maksim has been careful about exposing different group members to different areas of business, however, he placed a lot of trust in his long-term associate and second-in-command, **Aleksandr Viktorovich Ryzhenkov** (Aleksandr Ryzhenkov). Maksim started working with Aleksandr Ryzhenkov around 2013 while they were both still involved in the "Business Club" group. Their partnership endured, and they worked together on the development of a number of Evil Corp's most prolific ransomware strains. In 2016, Aleksandr Ryzhenkov, who is associated with the online moniker "Guester" (a pseudonym he has used while conducting operations on behalf of Evil Corp), sought to acquire internet bots in an Evil Corp operation targeting Switzerland-based targets. Since at least mid-2017, Aleksandr Ryzhenkov served as an interlocutor for Maksim with most of the Evil Corp members and oversaw operations of the cybercriminal group. In mid- 2017, Aleksandr Ryzhenkov targeted a New York-based bank. Following the December 2019 sanctions and indictment, Maksim and Aleksandr Ryzhenkov returned to operations targeting U.S.-based victims. In 2020, Aleksandr Ryzhenkov worked with Maksim to develop "Dridex 2.0."

Sergey Viktorovich Ryzhenkov (Sergey Ryzhenkov), **Aleksey Yevgenevich Shchetinin** (Shchetinin), **Beyat Enverovich Ramazanov** (Ramazanov), and **Vadim Gennadievich Pogodin** (Pogodin) are members of Evil Corp

who have provided general support to the cybercriminal group's activities and operations.

In 2019, Sergey Ryzhenkov, the brother of Aleksandr Ryzhenkov, helped to move Evil Corp operations to a new office. In 2020, after Evil Corp's sanctions designation and indictment, Sergey Ryzhenkov helped Aleksandr Ryzhenkov and Maksim develop "Dridex 2.0" malware. In 2017 through at least 2018, Shchetinin worked with several other Evil Corp members, including Denis Igorevich Gusev, Dmitriy Konstantinovich Smirnov, and Aleksei Bashlikov, to purchase and exchange millions of dollars' worth of virtual and fiat currencies. In early 2020, Pogodin played a crucial role in an Evil Corp ransomware attack, and in mid-2020, he contributed to an Evil Corp ransomware attack on a U.S. company.

OFAC designated Aleksandr Ryzhenkov, Sergey Ryzhenkov, Shchetinin, Ramazanov, and Pogodin pursuant to E.O. 13694, as amended, for having materially assisted, sponsored, or provided financial, material, or technological support, or goods or services in support of, Evil Corp, a person whose property and interests in property are blocked pursuant to E.O. 13694, as amended.

In addition to today's sanctions designations, the U.S. Department of Justice has unsealed an indictment charging Aleksandr Ryzhenkov with using the BitPaymer ransomware variant to target numerous victims throughout the United States. Aleksandr Ryzhenkov used a variety of methods to intrude into computers systems and used his ill-gotten access to demand millions of dollars in ransom. The Federal Bureau of Investigation's published a wanted poster for Aleksandr Ryzhenkov for his alleged involvement in ransomware attacks and money laundering activities. Also today, the United Kingdom designated 15 and Australia designated three Evil Corp members and affiliates.

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, financial institutions and other persons that engage in certain transactions or activities with the sanctioned persons may expose themselves to sanctions or be subject to an enforcement action. The prohibitions include the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any designated person, or the receipt of any contribution or provision of funds, goods, or services from any such person.

The power and integrity of OFAC sanctions derive not only from OFAC's ability to designate and add persons to the 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. F or 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.

Click here for more information on the individuals and entities designated today.

###
