

U.S. DEPARTMENT OF THE TREASURY

Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex



April 5, 2022

United States, International Partners Carry Out Multilateral Operation Targeting Russian Cybercrime

WASHINGTON – Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned the world's largest and most prominent darknet market, Hydra Market (Hydra), in a coordinated international effort to disrupt proliferation of malicious cybercrime services, dangerous drugs, and other illegal offerings available through the Russia-based site. The operation targeting Hydra was a collaborative initiative joined by the U.S. Department of Justice, Federal Bureau of Investigations, Drug Enforcement Administration, Internal Revenue Service Criminal Investigation, and Homeland Security Investigations. This action was enhanced by international cooperation with the German Federal Criminal Police, who today shut down Hydra servers in Germany and seized \$25 million worth of bitcoin.

"The global threat of cybercrime and ransomware that originates in Russia, and the ability of criminal leaders to operate there with impunity, is deeply concerning to the United States," said Secretary of the Treasury Janet L. Yellen. "Our actions send a message today to criminals that you cannot hide on the darknet or their forums, and you cannot hide in Russia or anywhere else in the world. In coordination with allies and partners, like Germany and Estonia, we will continue to disrupt these networks."

Darknets are Internet-based networks that individuals use special software to access in a manner designed to obscure the individuals' identity and their associated Internet activity. Marketplaces that reside on the darknet almost exclusively accept virtual currency as payment for a large range of illegal services and goods, including ransomware-as-a-service (RaaS). Virtual

currency is often the payment method of choice on darknet marketplaces because illicit actors who transact on the darknet often incorrectly believe virtual currencies to be an anonymous and untraceable means of exchange. Ransomware payments are also often demanded in virtual currency for similar reasons. Countering ransomware is a top priority of the Administration. Today's action supports the Administration's counter-ransomware lines of effort to disrupt ransomware infrastructure and actors in close coordination with international partners. The U.S. and German government's action today addresses the abuse of virtual currency to launder ransom payments.

Russia is a haven for cybercriminals. Today's action against Hydra and Garantex builds upon recent sanctions against virtual currency exchanges SUEX and CHATEX, both of which, like Garantex, operated out of Federation Tower in Moscow, Russia. Treasury is committed to taking action against actors that, like Hydra and Garantex, willfully disregard anti-money laundering and countering the financing of terrorism (AML/CFT) obligations and allow their systems to be abused by illicit actors. Wanton disregard for regulations and compliance by persons that run virtual currency exchanges will be rigorously investigated, and where appropriate, perpetrators will be held accountable. Additionally, the United States urges the international community to effectively implement international standards on AML/CFT in the virtual currency area, particularly regarding virtual currency exchanges. The virtual currency industry has a critical role to play in implementing appropriate AML/CFT and sanctions controls to prevent sanctioned persons and other illicit actors from exploiting virtual currencies to undermine the national security of the United States and our partners.

In addition to sanctioning Hydra, OFAC is identifying over [100 virtual currency addresses](#) associated with the entity's operations that have been used to conduct illicit transactions. Treasury is committed to sharing additional illicit virtual currency addresses as they become available.

As reflected in Executive Order (E.O.) 14067 of March 9, 2022, "Ensuring Responsible Development of Digital Assets," the Administration supports responsible innovation in digital assets, while prioritizing efforts to identify and mitigate illicit financing risks in the digital asset ecosystem. In the coming month, the Department of the Treasury will publish an updated

National Strategy to Combat Illicit Finance, which will highlight planned Treasury efforts to further combat the misuse of virtual currency and exchanges.

HYDRA MARKET: RUSSIA'S MOST PROMINENT DARKNET MARKET

Hydra was launched in 2015 and is the most prominent Russian darknet market, and the largest darknet market left in the world. Hydra's offerings have included ransomware-as-a-service, hacking services and software, stolen personal information, counterfeit currency, stolen virtual currency, and illicit drugs. Following a sale, Hydra's vendors have distributed illicit goods dropped anonymously in physical locations, sometimes buried or hidden in an inconspicuous location. Hydra's buyers received the location after purchase, often using virtual currency, and retrieved the illicit goods.

OFAC's investigation identified approximately \$8 million in ransomware proceeds that transited Hydra's virtual currency accounts, including from the Ryuk, Sodinokibi, and Conti ransomware variants. According to blockchain researchers, approximately 86 percent of the illicit Bitcoin received directly by Russian virtual currency exchanges in 2019 came from Hydra. Before today's action, Hydra's revenue had risen dramatically from under \$10 million in 2016, to over \$1.3 billion in 2020. This growth in profit is enabled by Hydra's association with Russian illicit finance. Additional details on the illicit financing risks associated with darknet markets can be found in the [National Money Laundering Risk Assessment](#) .

Hydra is being designated pursuant to E.O. 13694, as amended, for being responsible for or complicit in, or having engaged in, directly or indirectly, cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that have the purpose or effect of causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain.

VIRTUAL CURRENCY EXCHANGE GARANTEX

Garantex is a virtual currency exchange founded in late 2019 and originally registered in Estonia. Garantex allows customers to buy and sell virtual currencies using fiat currencies. The majority of Garantex's operations are carried out in Moscow, including at Federation Tower, and St. Petersburg, Russia, where other sanctioned virtual currency exchanges have also operated. Analysis of known Garantex transactions shows that over \$100 million in transactions are associated with illicit actors and darknet markets, including nearly \$6 million from Russian RaaS gang Conti and also including approximately \$2.6 million from Hydra. In February 2022, Garantex lost its license to provide virtual currency services after supervision by Estonia's Financial Intelligence Unit revealed critical AML/CFT deficiencies and found connections between Garantex and wallets used for criminal activity. Estonian authorities coordinated closely with the Treasury Department during this process. This is the [second time](#) in the last six months that Treasury has partnered with the Estonian government in relation to a virtual currency exchange facilitating malicious cyber activity. Despite losing its Estonian license to provide virtual currency services following the Estonian Financial Intelligence Unit's investigation, Garantex continues to provide services to customers through unscrupulous means.

Garantex is being designated today pursuant to E.O. 14024 for operating or having operated in the financial services sector of the Russian Federation economy.

Today's action also reinforces OFAC's recent [public guidance](#) to further cut off avenues for potential sanctions evasion by Russia, in support of the G7 leaders' commitment to maintain the effectiveness of economic measures. This guidance in the form of [Frequently Asked Question 1,021](#) makes clear that Treasury's expansive sanctions actions against Russia require all U.S. persons to comply with OFAC regulations, regardless of whether a transaction is denominated in traditional fiat currency or virtual currency. Sanctioned Russian persons are known to employ a wide variety of measures in their efforts to evade U.S. and international sanctions. As such, U.S. persons, wherever located, including firms that process virtual currency transactions, must be vigilant against attempts to circumvent OFAC regulations and must take


risk-based steps to ensure they do not engage in prohibited transactions. OFAC is closely monitoring any efforts to circumvent or violate Russia-related sanctions, including through the use of virtual currency, and is committed to using its broad enforcement authorities to act against violations and to promote compliance.

While most virtual currency activity is licit, virtual currencies can be used for illicit activity, including sanctions evasion through darknet markets, peer-to-peer exchangers, mixers, and exchanges. This includes the facilitation of ransomware schemes and other cybercrimes. Some virtual currency exchanges are exploited by malicious actors, but others, as is the case with Garantex, Suex, and Chatex, facilitate illicit activities for their own gains. Treasury continues to use its authorities against malicious cyber actors and their facilitators in concert with other U.S. departments and agencies, as well as our foreign partners, to disrupt financial nodes tied to ransomware payments, cyber-attacks, and other illicit activity.

SANCTIONS IMPLICATIONS

As a result of today's action, all property and interests in property of the individuals and entities 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, 50 percent or more by one or more blocked persons are also blocked. 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 are prohibited unless authorized by a general or specific license issued by OFAC, or exempt. These prohibitions include the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any blocked person and the receipt of any contribution or provision of funds, goods, or services from any such person.

[For identifying information on the individuals, entities, and property sanctioned or identified today, click here.](#)

For information on complying with sanctions applicable to virtual currency, see [OFAC's Sanctions Compliance Guidance for the Virtual Currency Industry here](#) . For FinCEN's recent

[alert identifying red flags on potential Russian sanctions evasion attempts, including through the use of cryptocurrency, see here.](#)

###