Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace

Press Release

Tuesday, April 5, 2022

For Immediate Release
Office of Public Affairs

Russian Resident Indicted on Conspiracy Charges Related to Operating Hydra Market

The Justice Department announced today the seizure of Hydra Market (Hydra), the world's largest and longest-running darknet market. In 2021, Hydra accounted for an estimated 80% of all darknet market-related cryptocurrency transactions, and since 2015, the marketplace has received approximately $5.2 billion in cryptocurrency.

The seizure of the Hydra servers and cryptocurrency wallets containing $25 million worth of bitcoin was made this morning in Germany by the German Federal Criminal Police (the Bundeskriminalamt), in coordination with U.S. law enforcement.

"The Justice Department will be relentless in our efforts to hold accountable those who violate our laws – no matter where they are located or how they try to hide their crimes," said Attorney General Merrick B. Garland. "Together with our German law enforcement partners, we have seized the infrastructure of the world's largest darknet market, but our work is far from over. We will continue to work alongside our international and interagency partners to disrupt and dismantle darknet markets, and to hold those who commit their crimes on the dark web accountable for their acts."

“The Department of Justice will not allow darknet markets and cryptocurrency to be a safe haven for money laundering and the sale of hacking tools and services,” said Deputy Attorney General Lisa O. Monaco. “Our message should be clear: we will continue to go after darknet markets and those who exploit them. Together with our partners in Germany and around the world, we will continue our work to disrupt the ecosystem that allows these criminal actors to operate.”

Hydra was an online criminal marketplace that enabled users in mainly Russian-speaking countries to buy and sell illicit goods and services, including illegal drugs, stolen financial information, fraudulent identification documents, and money laundering and mixing services, anonymously and outside the reach of law enforcement. Transactions on Hydra were conducted in cryptocurrency and Hydra’s operators charged a commission for every transaction conducted on Hydra.

In conjunction with the shutdown of Hydra, the department also announced criminal charges against Dmitry Olegovich Pavlov, 30, a resident of Russia, for conspiracy to distribute narcotics and conspiracy to commit money laundering, in connection with his operation and administration of the servers used to run Hydra.

“This coordinated action sends a clear message to anyone attempting to operate or support an online criminal enterprise under the cover of the dark web,” said U.S. Attorney Stephanie M. Hinds for the Northern District of California. “The dark web is not a place criminals can operate with impunity or hide from U.S. law enforcement, and we will continue to use our sophisticated tools and expertise to dismantle and disable darknet markets. This action also underscores the importance of international law enforcement collaboration. We thank German authorities and the Bundeskriminalamt, the German Federal Criminal Police Office, for its valued assistance in this case.”

“The darknet has been a key online marketplace for the sale of deadly drugs worldwide,” said Administrator Anne Milgram of the Drug Enforcement Administration (DEA). “The availability of illicit substances and money laundering services offered by Hydra threaten the safety and health of communities far and wide. Criminals on the darknet hide behind the illusion of anonymity, but DEA and our partners across the globe are watching. We will continue to investigate, expose, and take action against criminal networks no matter where they operate. I commend the extraordinary investigative efforts of DEA’s Miami Counternarcotic Cyber Investigations Task Force, Cyber Support Section, and Special Operations Division, and the teamwork from federal and international law enforcement partners that led to this action.”

“The Hydra darknet site provided a platform for criminals who thought they were beyond the reaches of law enforcement to buy and sell illegal drugs and services,” said Chief Jim Lee of IRS-Criminal Investigation. “Our Cyber Crimes Unit once again used their cryptocurrency tracking expertise to help take down this site and identify the criminal behind it. Denying criminals a space to operate freely to conduct their nefarious activities is the first step in stopping this activity from happening altogether.”

“The successful seizure of Hydra, the world's largest darknet marketplace, dismantled digital infrastructures which had enabled a wide range of criminals – including Russian cyber criminals, the cryptocurrency tumblers and money launderers that support them and others, and drug traffickers,” said FBI Director

Christopher Wray. “Today’s announcement is a testament to the strength and potency of our law enforcement partnerships here and around the world – and another example of our strategy to broadly target the entire illicit ecosystem that drives and enables crime.”

“The U.S. Postal Inspection Service is dedicated to protecting the United States mail from being used to transport illegal drugs and illicit goods available on the darknet,” said Chief Postal Inspector Gary R. Barksdale of the U.S. Postal Inspection Service National Headquarters. “The seizure of the criminal marketplace, Hydra Market, reflects the effective collaboration of law enforcement to stop criminal enterprises from their illicit activity. The Postal Inspection Service will continue to work with our federal partners to end these criminal organizations regardless of where they are.”

“The dismantling of the Hydra Market, the dark web’s largest supplier of illicit goods and services, sends a message to these electronic criminal kingpins that think they can operate with impunity,” said Special Agent in Charge Anthony Salisbury of Homeland Security Investigations (HSI) Miami. “HSI will continue to work with our U.S. and international law enforcement partners to target these transnational criminal organizations who attempt to manipulate the anonymity of the dark web to push their poison all over the world.”

According to the indictment, vendors on Hydra could create accounts on the site to advertise their illegal products, and buyers could create accounts to view and purchase the vendors’ products. Hydra vendors offered a variety of illicit drugs for sale, including cocaine, methamphetamine, LSD, heroin and other opioids. The vendors openly advertised their drugs on Hydra, typically including photographs and a description of the controlled substance. Buyers rated the sellers and their products on a five-star rating system, and the vendors’ ratings and reviews were prominently displayed on the Hydra site.

Hydra also featured numerous vendors selling false identification documents. Users could search for vendors selling their desired type of identification document – for example, U.S. passports or drivers’ licenses – and filter or sort by the item’s price. Many vendors of false identification documents offered to customize the documents based on photographs or other information provided by the buyers.

Numerous vendors also sold hacking tools and hacking services through Hydra. Hacking vendors commonly offered to illegally access online accounts of the buyer’s choosing. In this way, buyers could select their victims and hire professional hackers to gain access to the victims’ communications and take over the victims’ accounts.

Hydra vendors also offered a robust array of money laundering and so-called “cash-out” services, which allowed Hydra users to convert their bitcoin (BTC) into a variety of forms of currency supported by Hydra’s wide array of vendors. In addition, Hydra offered an in-house mixing service to launder and then process vendors’ withdrawals. Mixing services allowed customers, for a fee, to send bitcoin to designated recipients in a manner that was designed to conceal the source or owner of the bitcoin. Hydra’s money laundering features were so in-demand that some users would set up shell vendor accounts for the express purpose of running money through Hydra’s bitcoin wallets as a laundering technique.

Starting in or about November 2015, Pavlov is alleged to have operated a company, Promservice Ltd., also known as Hosting Company Full Drive, All Wheel Drive and 4x4host.ru, that administered Hydra's servers (Promservice). During that time, Pavlov, through his company Promservice, administered Hydra's servers, which allowed the market to operate as a platform used by thousands of drug dealers and other unlawful vendors to distribute large quantities of illegal drugs and other illicit goods and services to thousands of buyers, and to launder billions of dollars derived from these unlawful transactions.

As an active administrator in hosting Hydra's servers, Pavlov allegedly conspired with the other operators of Hydra to further the site's success by providing the critical infrastructure that allowed Hydra to operate and thrive in a competitive darknet market environment. In doing so, Pavlov is alleged to have facilitated Hydra's activities and allowed Hydra to reap commissions worth millions of dollars generated from the illicit sales conducted through the site.

The DEA's Miami Field Division, FBI, IRS-CI, U.S. Postal Inspection Service, and HSI investigated the case.

The U.S. investigation was conducted with support and coordination provided by the Department of Justice's multi-agency Special Operations Division and the Joint Criminal Opioid and Darknet Enforcement (JCODE) Team.

Trial Attorneys C. Alden Pelker and Christen M. Gallagher of the Criminal Division's Computer Crime and Intellectual Property Section and Assistant U.S. Attorneys Claudia A. Quiroz and Robert S. Leach for the Northern District of California are prosecuting the case.

In addition to the critically important efforts of the German Federal Criminal Police, significant assistance was provided by the Justice Department's Office of International Affairs and the U.S. Attorney's Office for the District of Columbia. Assistance was also provided by the Justice Department's National Cryptocurrency Enforcement Team.

An indictment is merely an allegation, and the defendant is presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

Updated April 5, 2022

Attachment
Pavlov Indictment [PDF, 5 MB]
Topic

Cybercrime

Press Release Number: 22-327