DeepDotWeb Administrator Pleads Guilty to Money Laundering Conspiracy

justice.gov/opa/pr/deepdotweb-administrator-pleads-guilty-money-laundering-conspiracy

Press Release

Wednesday, March 31, 2021

For Immediate Release
Office of Public Affairs

DeepDotWeb received over $8 million in kickbacks from purchases of fentanyl, firearms, and other contraband on Darknet marketplaces

An Israeli national pleaded guilty today for his role in operating DeepDotWeb (DDW), a website that connected internet users with Darknet marketplaces, where they purchased illegal firearms, malware and hacking tools, stolen financial data, heroin and fentanyl, and other contraband.

According to court documents, Tal Prihar, 37, an Israeli citizen residing in Brazil, owned and operated DDW along with co-defendant Michael Phan, 34, of Israel, beginning in October 2013. In addition to providing general information about the Darknet, DDW provided users with direct links to illegal Darknet marketplaces, which are not accessible through traditional search engines. For providing these links, Prihar and Phan received kickback payments from the marketplaces in the form of virtual currency, including approximately 8,155 bitcoins (worth approximately $8.4 million based on the bitcoin trading value at the time of the transactions). To conceal the nature and source of these illegal kickback payments, Prihar transferred the payments from his DDW bitcoin wallet to other bitcoin accounts and to bank accounts he controlled in the names of shell companies. DDW was seized by federal authorities in April 2019, and Prihar has agreed to forfeit $8,414,173.

“Tal Prihar served as a broker for illegal Darknet marketplaces — helping such marketplaces find customers for fentanyl, firearms, and other dangerous contraband — and profited from the illegal business that ensued,” said Acting Assistant Attorney General Nicholas L. McQuaid of the Justice Department’s Criminal Division. “This prosecution, seizure of the broker website, and forfeiture send a clear message that we are not only prosecuting the administrators of Darknet marketplaces offering illegal goods and services, but we will also bring to justice those that aim to facilitate and profit from them.”

“Tal Prihar today acknowledged his leadership role in operating a web site that served as a gateway to numerous dark web marketplaces selling fentanyl, heroin, firearms, hacking tools and other illegal goods,” said Acting U.S. Attorney Stephen R. Kaufman for the Western District of Pennsylvania. “Mr. Prihar and his codefendant extracted a fee from each customer routed to these illegal sites, profiting in the millions of dollars.”

“For six years, DeepDotWeb was a gateway to facilitate the illegal purchase of items to include dangerous drugs, weapons, and malicious software,” said Acting Special Agent in Charge Carlton Peeples of the FBI’s Pittsburgh Field Office. “Prihar profited as a byproduct from other people’s dangerous transactions and today’s guilty plea sends a message to other cyber actors across the globe who think the dark web is a safe haven. The FBI works with our local, state, federal and international partners regularly to dismantle illicit websites and go after those responsible for them.”

Prihar pleaded guilty to conspiracy to commit money laundering. He is scheduled to be sentenced on Aug. 2, and faces a maximum penalty of 20 years in prison. A federal district court judge will determine any sentence after considering the U.S. Sentencing Guidelines and other statutory factors.

The FBI’s Pittsburgh Field Office is investigating the case.

Assistant U.S. Attorney Jessica Lieber Smolar of the U.S. Attorney’s Office for the Western District of Pennsylvania and Trial Attorneys C. Alden Pelker of the Criminal Division’s Computer Crime and Intellectual Property Section and Alexander Gottfried of the Criminal Division’s Organized Crime and Gang Section are prosecuting the case.

The department thanks the French authorities as well as its law enforcement colleagues at the U.S. Postal Inspection Service, IRS, Brazilian Federal Police Cyber Division, Israeli National Police, Dutch National Police, Europol Darkweb Team, Federal Criminal Police Office of Germany, and National Crime Agency in the United Kingdom. Significant assistance was provided by the Justice Department’s Office of International Affairs.

This case was brought in conjunction with the Joint Criminal Opioid and Darknet Enforcement (J-CODE) Team. Established within the FBI’s Hi-Tech Organized Crime Unit, J-CODE is a U.S. Government initiative announced in January 2018, aimed at targeting drug trafficking, especially fentanyl and other opioids, on the Darknet. The J-CODE team brings together agents, analysts and professional staff with expertise in drugs, gangs, health care fraud and more. J-CODE entities, including the FBI, Drug Enforcement Administration, U.S. Postal Inspection Service, U.S. Customs and Border Protection, U.S. Immigration and Customs

Enforcement's Homeland Security Investigations, Department of Defense, Financial Crimes Enforcement Network and Department of Justice focus on disrupting the sale of drugs via the Darknet and dismantling criminal enterprises that facilitate this trafficking.

This prosecution also is a result of an Organized Crime Drug Enforcement Task Force (OCDETF) investigation. OCDETF identifies, disrupts, and dismantles high-level drug traffickers, money launderers, gangs, and transnational criminal organizations that threaten communities throughout the United States. OCDETF uses a prosecutor-led, intelligence-driven, multi-agency approach that leverages the strengths of federal, state, and local law enforcement agencies against criminal networks.

Updated March 31, 2021

Topics

Cybercrime

Opioids

Press Release Number: 21-287