Beat: News

United States Leads Seizure of One of the World's Largest Hacker Forums

Administrator Arrested

Washington, D.C., 12.04.2022, 16:12 Time

U.S. Department of Justice - Department of Justice
Office of Public Affairs
FOR IMMEDIATE RELEASE
Tuesday, April 12, 2022

The Department of Justice today announced the seizure of the RaidForums website, a popular marketplace for cybercriminals to buy and sell hacked data, and unsealed criminal charges against RaidForums' founder and chief administrator, Diogo Santos Coelho, 21, of Portugal. Coelho was arrested in the United Kingdom on Jan. 31, at the United States' request and remains in custody pending the resolution of his extradition proceedings.

Court records unsealed today indicate that the United States recently obtained judicial authorization to seize three domains that long hosted the RaidForums website. These domains were "raidforums.com," "Rf.ws," and "Raid.lol." According to the affidavit filed in support of these seizures, from in or around 2016 through February 2022, RaidForums served as a major online marketplace for individuals to buy and sell hacked or stolen databases containing the sensitive personal and financial information of victims in the United States and elsewhere, including stolen bank routing and account numbers, credit card information, login credentials and social security numbers.

"The takedown of this online market for the resale of hacked or stolen data disrupts one of the major ways cybercriminals profit from the large-scale theft of sensitive personal and financial information," said Assistant Attorney General Kenneth A. Polite, Jr. of the Justice Department's Criminal Division. "This is another example of how working with our international law enforcement partners has resulted in the shutdown of a criminal marketplace and the arrest of its administrator."

"Our interagency efforts to dismantle this sophisticated online platform – which facilitated a wide range of criminal activity – should come as a relief to the millions victimized by it, and as a warning to those cybercriminals who participated in these types of nefarious activities," said U.S. Attorney Jessica D. Aber for the Eastern District of Virginia. "Online anonymity was not able to protect the defendant in this case from prosecution, and it will not protect other online criminals either."

"The seizure of the RaidForums website – which facilitated the sale of stolen data from millions of people throughout the world – and the charges against the marketplace's administrator are a testament to the strength of the FBI's international partnerships," said Assistant Director in Charge Steven M. D'Antuono of the FBI's Washington Field Office said. "Cybercrime transcends borders, which is why the FBI is committed to working with our partners to bring cybercriminals to justice – no matter where in the world they live or behind what device they try to hide."

"This global investigation signifies the remarkable dedication of the U.S. Secret Service and highlights our partnerships with our foreign law enforcement counterparts essential to disrupting sophisticated networks of cyber criminals," said Special Agent in Charge Jason D. Kane of the U.S. Secret Service's Criminal Investigative Division. "This case exemplifies teamwork at all levels of law enforcement to stop these cyber criminals from defrauding citizens of the United States and in our partner countries."

Prior to its seizure, RaidForums members used the platform to offer for sale hundreds of databases of stolen data containing more than 10 billion unique records for individuals residing in the United States and internationally. At the time of its founding in 2015, RaidForums also operated as an online venue for organizing and supporting forms of electronic harassment, including by "raiding" – posting or sending an overwhelming volume of contact to a victim's online communications medium – or "swatting" – the practice of making false reports to public safety agencies of situations that would necessitate a significant, and immediate armed law enforcement response.

The seizure of these domains by the government will prevent RaidForums members from using the platform to traffic in data stolen from corporations, universities and governmental entities in the United States and elsewhere, including databases containing the

sensitive, private data of millions of individuals around the world.

In addition, a six-count indictment against Coelho was unsealed in the Eastern District of Virginia charging him with conspiracy, access device fraud and aggravated identify theft in connection with his role as the chief administrator of RaidForums. According to the indictment, between Jan. 1, 2015, and on or about Jan. 31, 2022, Coelho allegedly controlled and served as the chief administrator of RaidForums, which he operated with the help of other website administrators.

As administrators, Coelho and his co-conspirators are alleged to have designed and administered the platform's software and computer infrastructure, established and enforced rules for its users, and created and managed sections of the website dedicated to promoting the buying and selling of contraband, including a subforum titled "Leaks Market" that described itself as "[a] place to buy/sell/trade databases and leaks."

To profit from the illicit activity on the platform, RaidForums charged escalating prices for membership tiers that offered greater access and features, including a top-tier "God" membership status. RaidForums also sold "credits" that provided members access to privileged areas of the website and enabled members to "unlock," and download stolen financial information, means of identification, and data from compromised databases, among other items. Members could also earn credits through other means, such as by posting instructions on how to commit certain illegal acts.

According to the indictment, Coelho also personally sold stolen data on the platform, and directly facilitated illicit transactions by operating a fee-based "Official Middleman" service. For the Official Middleman service, Coelho allegedly acted as a trusted intermediary between RaidForums members seeking to buy and sell contraband on the platform, including hacked data. Notably, to create confidence amongst transacting parties, the Official Middleman service enabled purchasers and sellers to verify the means of payment and contraband files being sold prior to executing the transaction.

Assistant Attorney General Kenneth A. Polite, Jr. of the Justice Department's Criminal Division; U.S. Attorney Jessica D. Aber for the Eastern District of Virginia; Special Agent in Charge Jason D. Kane of the U.S. Secret Service's Criminal Investigative Division; and Assistant Director Steven M. D'Antuono of the FBI's Washington Field Office made the announcement.

Senior Trial Attorney Aarash Haghighat of the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) and Assistant U.S. Attorney Carina A. Cuellar for the Eastern District of Virginia are prosecuting the case against Coelho. The Justice Department's Office of International Affairs provided significant assistance throughout the criminal investigation.

The law enforcement actions against RaidForums and Coelho are the result of an ongoing criminal investigation by the FBI's Washington Field Office and the U.S. Secret Service. The department also thanks the support provided by Joint Cybercrime Action Taskforce (Europol), National Crime Agency (UK), Swedish Police Authority (Sweden), Romanian National Police (Romania), Judicial Police (Portugal), Internal Revenue Service Criminal Investigation, Federal Criminal Police Office (Germany) and other law enforcement partners.

Anyone that has any information regarding Coelho or RaidForums should file a complaint at ic3.gov with #RaidForums in the description.

Article online:
https://www.uspa24.com/bericht-20463/united-states-leads-seizure-of-one-of-the-worlds-largest-hacker-forums.html

Editorial office and responsibility:
V.i.S.d.P. & Sect. 6 MDStV (German Interstate Media Services Agreement):

submission of and access to third-party content. Liability for the content of a report lies solely with the author of such report.

Editorial program service of General News Agency:
UPA United Press Agency LTD
483 Green Lanes
UK, London N13NV 4BS
contact (at) unitedpressagency.com
Official Federal Reg. No. 7442619