Beat: News

United States Recovers Over $15 Million from Swiss Bank Accounts

Global Digital Advertising Fraud Scheme

New York, New York, 21.05.2022, 06:38 Time

USPA NEWS - Breon Peace, United States Attorney for the Eastern District of New York, announced today that $15,111,453.84 in illicit proceeds derived from an international digital fraud scheme has been transferred by Switzerland to the United States government pursuant to a Final Order of Forfeiture entered by United States District Judge Eric R. Komitee in the matter of United States v. Sergey Ovsyannikov, et al.

“This forfeiture is the largest international cybercrime recovery in the history of the Eastern District of New York and sends a powerful message to those involved in cyber fraud that there are no boundaries to prosecuting these bad actors and locating their ill-gotten assets wherever they are in the world,” stated United States Attorney Peace. “This Office will continue working with our law enforcement partners to take the economic gain out of crime through all available resources, including asset forfeiture, and protect the integrity of our marketplace.”

Mr. Peace thanked the Federal Bureau of Investigation, New York Field Office, and the New York City Police Department for their outstanding investigative work, the Swiss Federal Office of Justice, and the Justice Department’s Office of International Affairs for their invaluable assistance in this matter.

The Criminal Scheme

The internet is, in large part, freely available to users worldwide because it runs on digital advertising: website owners display advertisements on their sites and are compensated for doing so by intermediaries representing businesses seeking to advertise their goods and services to real human customers. In general, digital advertising revenue is based on how many users click or view the ads on those websites. The defendants in this case represented to others that they ran legitimate companies that delivered advertisements to real human internet users accessing real internet webpages. In fact, the defendants faked both the users and the webpages; they programmed computers they controlled to load advertisements on fabricated webpages, via an automated program, in order to fraudulently obtain digital advertising revenue.

Between December 2015 and October 2018, Sergey Ovsyannikov and Yevgeniy Timchenko, citizens of the Republic of Kazakhstan, and Aleksandr Isaev, a citizen of the Russian Federation, carried out a digital advertising fraud scheme known as “3ve.2 Template A” or “Eve.” The defendants used a global “botnet”-a network of malware-infected computers operated without the true owner’s knowledge or consent-to perpetrate digital advertising fraud. The defendants developed an intricate infrastructure of command-and-control servers to direct and monitor the infected computers and check whether a particular infected computer had been flagged by cybersecurity companies as associated with fraud. By using this infrastructure, the defendants accessed more than 1.7 million infected computers belonging to individuals and businesses in the United States and elsewhere, including more than 1,500 at residences and businesses in the Eastern District of New York—and used hidden browsers on those infected computers to download fabricated webpages and load ads onto those fabricated webpages.

As a result of this scheme, the defendants falsified billions of ad views and spoofed more than 86,000 domains associated with online publishers, causing businesses to pay more than $29 million for ads that were never actually viewed by real human internet users and diverting that money away from the real online publishers for whom it was intended. The $15.1 million recovered from financial accounts in Switzerland were the proceeds of this digital advertising fraud scheme.

Ovsyannikov was arrested in October 2018 in Malaysia and extradited to the United States. Timchenko was arrested in November 2018 in Estonia and extradited to the United States. Both pleaded guilty and have been sentenced. Isaev remains at large.

Following the arrest of Ovsyannikov by Malaysian authorities, U.S. law enforcement authorities, in conjunction with various private sector companies, began the process of dismantling the criminal cyber infrastructure utilized in the botnet-based scheme, which involved computers infected with malicious software known in the cybersecurity community as “Kovter.” The FBI executed seizure warrants to sinkhole 23 internet domains used to further the charged botnet-based scheme or otherwise used to further the Kovter

botnet. The FBI also executed search warrants at 11 different U.S. server providers for 89 servers related to the charged botnet-based scheme or Kovter.

Forfeiture matters related to the sentencings in this case were handled by Assistant United States Attorney Brendan G. King and former Assistant United States Attorney Karin K. Orenstein of the Office's Asset Recovery Section. Assistant United States Attorneys Saritha Komatireddy, Artie McConnell, and Alexander F. Mindlin are in charge of the criminal prosecution.

Thank you for reading my article. These are merely my thoughts and insights based on the facts. I use only verified sources. No fake news here. I write about a variety of subjects, mainly things I want to research and know more about. You can check out my website – Small Village Life at smallvillagelife.com, where I share useful articles and news.

Wendy writes for the United States Press Agency and is a former columnist with the Fulton County Expositor, Wauseon, Ohio.

Source: Department of Justice, U.S. Attorney's Office, Eastern District of New York press release May18, 2022

Article online:
https://www.uspa24.com/bericht-20825/united-states-recovers-over-15-million-from-swiss-bank-accounts.html

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

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