The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

U.S. Sanctions Russian Cybercrime Outfit 'Evil Corp'

The U.S. government is offering a $5 million reward for the capture of Evil Corp's leader.

By Bloomberg

December 05, 2019

The U.S. government said Evil Corp was behind $100 million of stolen funds. **Christopher Schirner / Flickr (CC BY-SA 2.0)**

The U.S. Treasury Department said it would sanction a Russian group known as "Evil Corp" and its leaders for cyber-thefts at hundreds of financial institutions around the world that total more than $100 million.

The targets include the group's leader, identified as Maksim Yakubets. The U.S. said he also worked for the Russian Federal Security Service, an intelligence agency known as the FSB that's already under U.S. sanctions, and was directed to work on projects for the Russian state as of 2017.

The sanctions were accompanied by indictments of Yakubets filed in federal court in Nebraska and Pennsylvania, charging him with conspiracy and fraud involving Bank of America and regional U.S. lenders. He is at large, and the State Department offered a $5 million reward for information leading to his capture.

Yakubets "is not the first cybercriminal to be tied to the Russian government," the Treasury Department said in a statement, citing the 2017 indictment of two FSB officers and conspirators for compromising "millions" of Yahoo email accounts. "The United States Government will not tolerate this type of activity by another government or its proxies and will continue to hold all responsible parties accountable."

Related article: Russia's FSB Linked to $450M Bitcoin Disappearance – BBC

Another top Evil Corp leader, Igor Turashev, was also sanctioned and indicted.

"For over a decade, Maksim Yakubets and Igor Turashev led one of the most sophisticated transnational cyber-crime syndicates in the world," U.S. Attorney Scott Brady said in a statement.

Evil Corp has used malware called Dridex to harvest log-in credentials from banks and financial institutions in more than 40 countries, the Treasury Department said. Prosecutors said in the Nebraska indictment that the malware affected thousands of computers.

"Our goal is to shut down Evil Corp, deter the distribution of Dridex, target the 'money mule' network used to transfer stolen funds, and ultimately to protect our citizens from the group's criminal activities," Treasury Secretary Steven Mnuchin said in the statement.

Senior Treasury officials said the U.S. action was coordinated with a crackdown on Evil Corp and Dridex by the U.K., and also in cooperation with countries and places targeted by the group including Italy, Australia, the United Arab Emirates, Canada, France, India, Hong Kong and Malaysia.

Dridex, also known as Bugat and Cridex, often reaches victims through phishing emails. It is "a multifunction malware package that automates the theft of confidential personal and financial information, such as online banking credentials, from infected computers through the use of keystroke logging and web injects," according to the indictment.

In October of 2015, U.S. prosecutors indicted Moldovan national Andrey Ghinkul for cyber-attacks using Dridex, which Justice called "a sophisticated malware package designed to steal banking and other credentials from infected computers."

Dridex can be used by hackers as a tool for compromising credentials and gaining access to financial information. It is "one of the most prevalent eCrime malware families," according to a July report by the cybersecurity firm Crowdstrike, which said that Dridex was used significantly in 2015 and 2016.

Original url:
https://www.themoscowtimes.com/2019/12/05/us-sanctions-russian-cybercrime-outfit-evil-corp-a68499