

US indicts Russian suspect in huge botnet takedown

April 21 2017



During any 24-hour period, prosecutors say the botnet generated and distributed more than 2,500 unsolicited spam emails that advertised various criminal schemes

A Russian under arrest in Spain has been slapped with an indictment in the United States, accused of controlling one of the world's top generators of spam and online extortion, officials said Friday.

Peter Levashov, from Saint Petersburg, a 36-year-old who goes by a string of names, was arrested at Barcelona airport on April 7 by Spanish authorities acting on a US warrant. The United States is now seeking his extradition.

A US federal grand jury returned the eight-count indictment in the northeastern state of Connecticut on Thursday. The charges include fraud, identity theft and conspiracy.

If convicted at trial, he is likely to spend years in a US federal prison.

Prosecutors accuse the purported hacker of controlling the Kelihos network of tens of thousands of infected computers, stealing personal data and renting the network out to others to send spam emails by the millions and extort ransoms.

Levashov could allegedly remotely order the delivery of fraudulent spam and malicious computer viruses on behalf of whoever would pay him to do so.

US officials say he was proud of his work and advertised the ever-improving effectiveness of his spam services with a standard price list. For legal ads, he charged \$200 per million spam emails. For illegal scams and phishing attacks, it was \$500 per million.

To help someone with a stock manipulation, he allegedly wanted a deposit of \$5,000-\$10,000 to share his list of 25 million traders. He also demanded 5 percent of the gains made on the stock.

During any 24-hour period, prosecutors say the botnet generated and distributed more than 2,500 unsolicited spam emails that advertised various criminal schemes.

The US Justice Department shut down the botnet on April 10.

Levashov has not been tied to Russian interference in last year's US presidential election.

But his operation depended on sending spam emails that allowed hackers to penetrate the computers of the Democratic Party to steal data. That was exactly the kind of botnet service he allegedly sold to criminals.

© 2017 AFP

Citation: US indicts Russian suspect in huge botnet takedown (2017, April 21) retrieved 27 April 2024 from <https://phys.org/news/2017-04-russian-accused-spam-indicted.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.