

Prosecutor: Russian man's computer linked to hacking scheme (Update)

August 15 2016, by Martha Bellisle



In this June 5, 2013, file photo, attorney John Henry Browne listens to questions from reporters at Joint Base Lewis-McChord in Washington state. Browne will be representing accused Russian computer hacker Roman Seleznev as jury selection for a federal trial begins Monday, Aug. 15, 2016, in Seattle. Prosecutors accuse Seleznev of hacking into U.S. business computer systems, mostly pizza restaurants in Washington state, and selling credit card data on underground internet forums. (AP Photo/Ted S. Warren, File)

When federal agents arrested a Russian man in the Maldives in 2014, they found 1.7 million stolen credit card numbers on his laptop computer, a federal prosecutor told the jury Monday during opening statements.

That was "1.7 million people who had eaten at the wrong restaurant and their personal information was sitting on that man's computer," Assistant U.S. Attorney Seth Wilkinson said of Roman Seleznev. He had collected the credit card numbers by hacking into restaurants in Washington and other states, Wilkinson said.

"The evidence will show that for seven years, the defendant was one of the largest traffickers of stolen credit card numbers in the world," Wilkinson said.

Seleznev's lawyer, John Henry Browne, said he will decide by Tuesday morning whether he will make an opening statement.

Browne plans to argue that prosecutors have failed to adequately connect Seleznev with the computer hacks that hit more than 200 businesses over several years. Browne also will likely argue that the agents who took possession of Seleznev's computer opened it without a warrant and may have tampered with or altered some of its data.

The judge had previously refused to grant a motion to suppress the information taken from the computer, but said Browne can make the argument to the jury.

Seleznev's trial in U.S. District Court is expected to run more than two weeks.

After the jury left for the day, Browne told U.S. District Judge Richard Jones that he objected to Wilkinson's mention of Seleznev's arrest in the

Maldives. Browne and the Russian government had argued that the arrest was a kidnapping that violated international law. But Jones had ruled in earlier hearings that the kidnapping claim could not be brought up during trial.

Wilkinson's statements about the Maldives may be grounds for a mistrial motion, Browne said.

The prosecutor's opening statement laid out the history of the investigation into seven years of hacking.

Agents started on Seleznev's trail in 2010 after a deli in Idaho was hacked and credit card data was stolen, Wilkinson said. The U.S. Secret Service and local detectives traced the hack to a computer server in Russia, he said.

The agents found some of the stolen credit card numbers being sold on a website being run by a hacker who used the nickname Track2, he said.

Detective work eventually linked the point-of-sale hacking to stolen card sales and then to a computer server in Virginia, where some of the stolen data was stored.

A search of that server found 170,000 stolen credit card numbers, but a review of its internet activity also revealed personal email activity of Roman Seleznev, he said.

It showed that Seleznev had purchased a plane ticket in his own name, had bought flowers for his wife and had participated on an online poker club, Wilkinson said.

"The agent found Roman Seleznev's fingerprints all over the crime scene," Wilkinson said. "This trial will be about exposing the

fingerprints, that the defendant is Track2."

Seleznev was indicted in 2011, but the agents couldn't arrest him in Russia. But in 2014 when they learned he was on vacation in the Maldives, they worked with local police to arrest him at the airport.

He was brought back to the U.S. to face an indictment that was amended to include 40 felony counts that include bank and wire fraud, hacking and identity theft, Wilkinson said.

© 2016 The Associated Press. All rights reserved.

Citation: Prosecutor: Russian man's computer linked to hacking scheme (Update) (2016, August 15) retrieved 18 April 2024 from <https://phys.org/news/2016-08-russian-trial-lucrative-hacking-scheme.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.