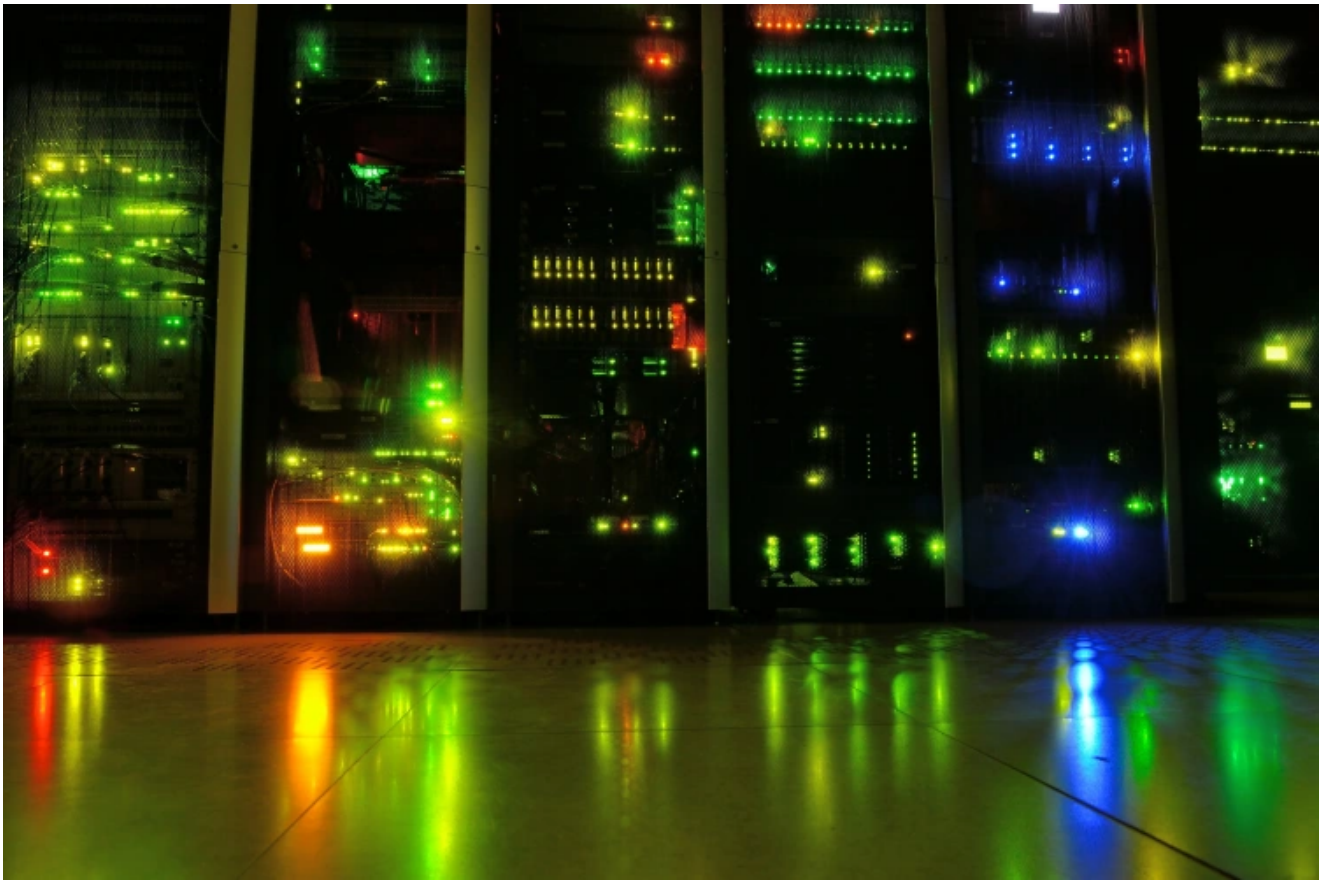
Related news

cyberscoop.com/doj-kelihos-botnet-peter-levashov-severa/

April 10, 2017



government

DOJ moves to topple Kelihos, one of the world's largest botnets

Photo by Tristan Schmurr (Flickr/CC BY 2.0)
Written by Patrick Howell O'Neill
Apr 10, 2017 | CYBERSCOOP
The Department of Justice announced Monday an effort to take down a global network of over 100,000 enslaved computers under the control of Peter Yuryevich Levashov.

Levashov, also known as Peter Severa, was known as one of the world's most prolific and long-reigning kings of spam. A citizen of Russia, he was arrested in Spain earlier this week.

The network, known as the Kelihos botnet, has been in operation since 2010, targeting Microsoft Windows machines for infection. The result was millions of spam emails, pump-and-dump schemes to illegally profit off stocks, mass password theft and the spreading of

malware, according to the DOJ. Roughly 5 percent to 10 percent of Kelihos victims reside in the United States, according to the Justice Department.

“The ability of botnets like Kelihos to be weaponized quickly for vast and varied types of harms is a dangerous and deep threat to all Americans, driving at the core of how we communicate, network, earn a living and live our everyday lives,” said acting Assistant Attorney General Kenneth Blanco.

Levashov was first indicted over a decade ago by U.S. authorities on charges of email and wire fraud for allegedly using spam to promote profitable pump-and-dump penny stock schemes.

He was charged again in 2009 for allegedly operating the Storm botnet, another spam behemoth and a predecessor to Kelihos.

This week’s arrest was made possible because the FBI learned just last month that Levashov was going to leave his home in Russia, a country without extradition to the United States, to spend several weeks in Spain. The details about how the FBI came into that information remain unknown.

Levashov was connected to Kelihos by the FBI by connecting IP addresses used to operate the botnet that was also used by email and other online accounts under the name of Pete Levashov, a web programmer in Russia.

Levashov regularly used the same addresses to commit crime. To connect the dots, the FBI obtained Levashov’s records from companies including Google, Apple, WebMonkey and Foursquare.

The operation against Kelihos is global in scale, according to the DOJ, who worked in concert with law enforcement around the world. The department cited the newly amended Rule 41 as the source of authorization for the botnet’s disruption.

“Let me emphasize that there was no entry into the computers to take information using this warrant,” a Justice Department official said during a call with reporters. “This was merely used as a disruption technique against this botnet, it was not a search warrant against the computers that were part of the botnet.”

The FBI worked with CrowdStrike, a private security company, and Shadowserver Foundation, a volunteer group of information security experts, to deploy a sinkhole attack to sever the communication networks between criminal directors and infected computers. The DOJ cautioned that, as is normal in offensives against large botnets, the operation against Kelihos will not be 100 percent complete for some time to come.

“This isn’t an operation where you can throw a switch and turn off the botnet,” a Justice Department official said. “There is a lag time. We’ll continue our operation to have the most impact we can on this particular botnet. So far the signs are very good that we’ve had a significant disruption of this botnet.”

You can read the criminal complaint and application for a search warrant below:
[documentcloud url=”http://www.documentcloud.org/documents/3549532-Signed-Application-for-Search-Warrant-Redacted-0.html” responsive=true sidebar=false text=false pdf=false]
[documentcloud url=”http://www.documentcloud.org/documents/3549535-Dkt-1-Complaint-0.html” responsive=true sidebar=false text=false pdf=false]