How Russian Spam King Peter Levashov Was Arrested, and His Kelihos Botnet Dismantled

By Garrett M. Graff

Published: 2017-04-11 · Archived: 2026-05-01 02:18:03 UTC

One of the world's most notorious spammers appears to have been tripped up by a basic cybersecurity no-no, according to the FBI: He used the same log-in credentials to both run his criminal enterprise and also log into sites like iTunes.

The Justice Department announced Monday that it had successfully targeted a man prosecutors called "one of the world's most notorious criminal spammers," a Russian hacker known as Peter Yuryevich Levashov, also known as Peter Severa, or "Peter of the North." Levashov had long run the Kelihos botnet, a global network of infected computers that collectively flooded email inboxes worldwide with spam, stole banking credentials from infected users, and spread malware across the internet.

Spanish authorities arrested Levashov, who normally resides in St. Petersburg, Russia, while he was on vacation with his family. Rumors had swirled over the weekend, sourced only to a vague report on the Russian propaganda network RT, that he'd been involved in that country's meddling with the 2016 US presidential election, but there was no hint of that in Monday's Justice Department complaint, which focused instead on Levashov's role in developing and running one of the internet's most pernicious and longest-running botnets. Levashov's operation had infected as many as 100,000 computers worldwide, roughly five to ten percent of which were inside the United States.

Prosecutors described Kelihos as a sophisticated malware variant that harvested user credentials from victim computers, and was used to send massive quantities of spam emails. The complaints and court orders associated with the case also laid out details of how Levashov operated his business, offering a million spam messages promoting "legal" products such as "adult, mortgage, leads, pills, replics [i.e., counterfeit goods], etc." for just $200, while that price went to $300 per million messages for "Job spam," that is, messages that attempted to recruit job seekers into fraudulent positions, including "money mules" who would help launder stolen money and goods. According to the Justice Department, Levashov also offered to deploy his network on behalf of online fraudsters to execute phishing attacks for $500 per million messages.

As part of the operation, security researchers and the FBI teamed up to dismantle the Kelihos botnet itself, targeting three domains used to run the network—gorodkoff.com, goloduha.info, and combach.com---and redirecting traffic from infected computers to new servers controlled by authorities and the ShadowServer Foundation, a volunteer anti-cybercrime group, a process that's known in cybersecurity circles as "sink-holing."

Cracking Down

The arrest of Levashov---and the complex, sophisticated assault on his long-running botnet---marked another victory in the US government's rising war against Russian aggression in cyberspace, coming just weeks after

another Justice Department indictment charged both Russian criminals and intelligence officer with conspiring to hack Yahoo's user database.

It also, for the time being at least, perhaps marked the end of one of the most powerful spam networks on the internet, a global network of malware-infected computers that had proven uniquely difficult to dismantle, reappearing multiple times and evolving even as its chief output---multitudes upon multitudes of unwanted junk emails advertising Viagra, adult entertainment, and, at worst, phishing emails that spread even more malware---continued unabated for the better part of a decade.

"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 Kenneth Blanco, the acting assistant attorney general overseeing the Justice Department's criminal division.

The case also marks one of the first times that the Justice Department has acknowledged using what's known as "Rule 41," a controversial change to federal criminal procedures that took effect last December and allows the government to seek powerful search warrants to investigate cybercrime no matter where infected computers might be physically located. (The Justice Department, though, was quick to caution Monday that it didn't actually use warrants to penetrate any infected computer, merely to help attack the botnet nationwide.)
