US convicts Russian national behind Kelihos botnet crypting service

bleepingcomputer.com/news/security/us-convicts-russian-national-behind-kelihos-botnet-crypting-service/

Sergiu Gatlan

By
Sergiu Gatlan

- June 16, 2021
- 12:22 PM
- 0

Russian national Oleg Koshkin was convicted for charges related to the operation of a malware crypter service used by the Kelihos botnet to obfuscate malware payloads and evade detection.

Koshkin has been detained since he was arrested in California in September 2019, and he is facing a maximum penalty of 15 years in prison after September 20, 2021, when his sentencing is due.

Estonian national Pavel Tsurkan, his co-defendant, also pled guilty today via videoconference to charges of aiding and abetting hackers to infect victim computers worldwide with malicious software, including ransomware.

Monthly payments of $3,000 for malware crypting services

Koshkin operated Crypt4U.com, Crypt4U.net, fud.bz, fud.re, and other websites that promised to render malware (e.g., botnets, remote-access trojans, keyloggers, credential stealers, and cryptocurrency miners) fully undetectable by almost all major providers of antivirus solutions.

"In particular, Koshkin worked with Peter Levashov, the operator of the Kelihos botnet, to develop a system that would allow Levashov to crypt the Kelihos malware multiple times each day," the Department of Justice said.

"Koshkin provided Levashov with a custom, high-volume crypting service that enabled Levashov to distribute Kelihos through multiple criminal affiliates.

"Levashov used the Kelihos botnet to send spam, harvest account credentials, conduct denial of service attacks, and distribute ransomware and other malicious software."

The Kelihos maintainer paid Koshkin roughly $3,000 per month for his services between May 2014 and April 2017 per the criminal complaint when Levashov was arrested in Spain.

Kelihos botnet, one of the largest of its time

The Kelihos botnet, active since at least 2010 and one of the largest when it was taken down in 2017, was used by its operators and other cybercriminals who rented it to send millions of spam messages per hour.

US authorities said at the time that Levashov was renting the botnet's spamming capabilities for prices from $100 to $300, according to court documents,

The botnet was targeted by three takedown attempts in consecutive years, in 2011, 2012, and 2013, and was finally taken down in April 2017.

When the FBI finally dismantled it, the Kelihos botnet was known to control at least 60,000 compromised computers worldwide.

"By operating a website that was intended to hide malware from antivirus programs, Koshkin provided a critical service that enabled other cyber criminals to infect thousands of computers around the world," Acting U.S. Attorney Leonard C. Boyle for the District of Connecticut said.

"The defendant designed and operated a service that was an essential tool for some of the world’s most destructive cybercriminals, including ransomware attackers," added Acting Assistant Attorney General Nicholas L. McQuaid of the Justice Department's Criminal Division.

Related Articles:

Microsoft detects massive surge in Linux XorDDoS malware activity

Microsoft: Sysrv botnet targets Windows, Linux servers with new exploits

New cryptomining malware builds an army of Windows, Linux bots

Emotet botnet switches to 64-bit modules, increases activity

New stealthy BotenaGo malware variant targets DVR devices