Russian National Convicted of Charges Relating to Kelihos Botnet

justice.gov/opa/pr/russian-national-convicted-charges-relating-kelihos-botnet

June 16, 2021

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Wednesday, June 16, 2021

A federal jury in Connecticut convicted a Russian national on Tuesday for operating a “crypting” service used to conceal “Kelihos” malware from antivirus software, enabling hackers to systematically infect victim computers around the world with malicious software, including ransomware.

According to court documents and evidence introduced at trial, Oleg Koshkin, 41, formerly of Estonia, operated the websites “Crypt4U.com,” “fud.bz” and others. The websites promised to render malicious software fully undetectable by nearly every major provider of antivirus software. Koshkin and his co-conspirators claimed that their services could be used for malware such as botnets, remote-access trojans, keyloggers, credential stealers and cryptocurrency miners.

“The defendant designed and operated a service that was an essential tool for some of the world’s most destructive cybercriminals, including ransomware attackers,” said Acting Assistant Attorney General Nicholas L. McQuaid of the Justice Department's Criminal Division. “The verdict should serve as a warning to those who provide infrastructure to

cybercriminals: the Criminal Division and our law enforcement partners consider you to be just as culpable as the hackers whose crimes you enable — and we will work tirelessly to bring you to justice."

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. 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. At the time it was dismantled by the FBI, the Kelihos botnet was known to include at least 50,000 compromised computers around the world.

"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," said Acting U.S. Attorney Leonard C. Boyle for the District of Connecticut. "We will investigate and prosecute the individuals who aid and abet cyber criminals as vigorously as we do the ones who actually hit the 'send' button on viruses and other malicious software."

"Koshkin and his associates knowingly provided crypting services designed to help malicious software bypass anti-virus software," said Special Agent in Charge David Sundberg of the FBI's New Haven Division. "The criminal nature of the Crypt4U service was a clear threat to the confidentiality, integrity, and availability of computer systems everywhere. We at the FBI will never stop pursuing those like Koshkin for perpetrating cyber crimes and threats to the public at large."

Koshkin was arrested in California in September 2019 and has been detained since his arrest. He faces a maximum penalty of 15 years in prison and is scheduled to be sentenced on Sept. 20.

Koshkin's co-defendant, Pavel Tsurkan, is charged with conspiring to cause damage to 10 or more protected computers, and aiding and abetting Levashov in causing damage to 10 or more protected computers.

Levashov was arrested by the Spanish National Police in April 2017 and extradited to the United States. In September 2018, he pleaded guilty to one count of causing intentional damage to a protected computer, one count of conspiracy, one count of wire fraud, and one count of aggravated identity theft.

The FBI's New Haven Division investigated the case through its Connecticut Cyber Task Force.

Assistant U.S. Attorney Edward Chang of District of Connecticut, and Senior Counsel Ryan K.J. Dickey of the Criminal Division's Computer Crime and Intellectual Property Section are prosecuting the case with assistance from the Criminal Division's Office of International Affairs. The Estonian Police and Border Guard Board also provided significant assistance.

This case is part of the Department of Justice's Ransomware and Digital Extortion Task Force, which was created to combat the growing number of ransomware and digital extortion attacks. As part of the Task Force, the Criminal Division, working with the U.S. Attorneys' Offices, prioritizes the disruption, investigation, and prosecution of ransomware and digital extortion activity by tracking and dismantling the development and deployment of malware, identifying the cybercriminals responsible, and holding those individuals accountable for their crimes. The department, through the Task Force, also strategically targets the ransomware criminal ecosystem as a whole and collaborates with domestic and foreign government agencies as well as private sector partners to combat this significant criminal threat.