Russian National Sentenced for Providing Crypting Service for Kelihos Botnet

Press Release

Thursday, December 9, 2021

For Immediate Release
Office of Public Affairs

A Russian national was sentenced today to 48 months in prison for operating a “crypting” service used to conceal the Kelihos malware from antivirus software, which enabled hackers to systematically infect approximately hundreds of thousands of victim computers around the world with malicious software, including ransomware.

According to court documents, Oleg Koshkin, 41, was convicted by a federal jury on June 15 of one count of conspiracy to commit computer fraud and abuse and one count of computer fraud and abuse.

“The defendant provided a critical service used by cybercriminals to evade one of the first lines of cybersecurity defense, antivirus software,” said Assistant Attorney General Kenneth A. Polite Jr. of the Justice Department’s Criminal Division. “Cybercriminals depend on services like these to infect computers around the world with malware, including ransomware. The Criminal Division and our law enforcement partners are committed to investigating and prosecuting anyone who criminally operates these services to the fullest extent of the law."

“Koshkin’s unscrupulous websites provided a vital service to cyber criminals, allowing them to hide their malware from antivirus programs and use it to infect thousands of computers all over the world,” said Acting U.S. Attorney Leonard C Boyle of the District of Connecticut. “We will continue to work closely with our investigative partners to root out and prosecute individuals involved across the ransomware spectrum, wherever they try to hide.”

“Today’s sentencing of Oleg Koshkin serves as another example of the risk and consequences awaiting those who choose to commit cybercrimes against the American public,” said Special Agent in Charge David Sundberg of the FBI’s New Haven Division. “For years, Koshkin and his co-conspirators worked to evade our most basic cyber defenses in order to spread malware on a truly global scale. While our work to bring Koshin to justice comes to a close, the FBI will continue to tirelessly defend our country from the ever-evolving cyber threats posed by criminals, terrorists and hostile nation-states.”

According to court documents and evidence presented at trial, Koshkin 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.

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. In September 2018, Levashov pleaded guilty to various fraud, conspiracy, computer crime and identity theft offenses.

Koshkin provided Levashov with a custom, high-volume crypting service that enabled Levashov to distribute Kelihos through multiple criminal affiliates. The Kelihos botnet was used by Levashov to send spam, harvest account credentials, conduct denial of service attacks, and to distribute ransomware and other malicious software. According to evidence presented at Koshkin’s sentencing, Kelihos relied on the crypting services provided by Crypt4U from 2014 until Levashov’s arrest in April 2017; and just in the last four months of that conspiracy, Kelihos infected approximately 200,000 computers around the world.

Koshkin’s co-defendant, Pavel Tsurkan, pleaded guilty on June 16 to one count of causing damage to a protected computer, an offense that carries a maximum term of 10 years in prison. He is awaiting sentencing.

The FBI’s New Haven Field Office investigated the case through its Connecticut Cyber Task Force.

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

The Department of Justice announced in April the creation of the Ransomware and Digital Extortion Task Force 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.

Updated December 9, 2021

Topic

Cybercrime

Press Release Number: 21-1227