Russian and Moldovan National Pleads Guilty to Operating Illegal Botnet Proxy Service that Infected Tens of Thousands of Internet-Connected Devices Around the World

justice.gov/usao-pr/pr/russian-and-moldovan-national-pleads-guilty-operating-illegal-botnet-proxy-service

November 14, 2023

Press Release

SAN JUAN, Puerto Rico – A Russian and Moldovan national pled guilty to three counts of violating 18 U.S.C. § 1030(a)(5)(A) Fraud and Related Activity in Connection with Computers.

The FBI today revealed US law enforcement's dismantlement of a botnet proxy network and its infrastructure associated with the IPStorm malware.

According to online reports, the botnet infrastructure had infected Windows systems then further expanded to infect Linux, Mac, and Android devices, victimizing computers and other electronic devices around the world, including in Asia, Europe, North America and South America.

In connection with the operation of that IPStorm malware and botnet proxy service, on September 18, 2023, Sergei Makinin, a Russian and Moldovan national, pled guilty to three counts of violating 18 U.S.C. § 1030(a)(5)(A), knowingly causing the transmission of a program that intentionally caused damage without authorization to protected computers. Each count of conviction carries a statutory maximum of ten years in prison. A federal district court judge will determine any sentence after considering the U.S. Sentencing Guidelines and other statutory factors.

According to court documents, from at least June 2019 through December 2022, Makinin developed and deployed malicious software to hack thousands of Internet-connected devices around the world, including in Puerto Rico. Makinin controlled these infected devices as part of an extensive botnet, which is a network of compromised devices. The main purpose of the botnet was to turn infected devices into proxies as part of a for-profit scheme, which made access to these proxies available through Makinin's websites, proxx.io and proxx.net. Through those websites, Makinin sold illegitimate access to the infected, controlled devices to customers seeking to hide their Internet activities. A single customer could pay hundreds of dollars a month to route traffic through thousands of infected computers. Makinin's publicly-accessible website advertised that he had over 23,000 "highly anonymous" proxies from all over the world. Makinin acknowledged that he gained at least $550,000 from the scheme. Pursuant to the plea agreement, Makinin will forfeit cryptocurrency wallets linked to the offense.

"This investigation shows that we will use every lawful tool at our disposal to disrupt cybercriminals, regardless of their location," said U.S. Attorney Stephen Muldrow. "This case serves as a warning that the reach of the law is long, and criminals anywhere who use computers to commit crimes may end up facing the consequences of their actions in places they did not anticipate."

"It is no secret that in present times, much criminal activity is conducted or enabled through cybernetic means. Cybercriminals seek to remain anonymous and derive a sense of security because they hide behind keyboards, often thousands of miles away from their victims," said Joseph González, Special Agent in Charge of the FBI's San Juan Field Office. "The FBI's cyber mission has been to impose risk and consequences on our adversaries, ensuring cyberspace is no safe space for criminal activity. This case is one example of how we are doing just that, and I'd like to thank the DOJ's Computer Crime and Intellectual Property Section, the US Attorney's Office for the District of Puerto Rico, and the FBI San Juan Cyber Team for their meticulous and relentless work in this case."

The scope of the law enforcement dismantlement was limited to disabling the defendant's infrastructure and did not extend to the information of the owners and users of the computers. The FBI emphasizes the importance of keeping computers updated with the latest security patches and operating systems.

The case was investigated by the FBI San Juan Cyber Team, with cooperation from the FBI legal attaché office in Madrid in coordination with the Spanish National Police-Cyber Attack Group; and the FBI Legal Attaché office in Santo Domingo, in coordination with the Dominican National Police-Interpol and Dominican National Police-International Organized Crime Division, and Ministry of the Interior and Police-Immigration Directorate. Valuable assistance was provided by the National Cyber-Forensics and Training Alliance

(NCFTA.net), including Bitdefender DRACO Team, Anomali Threat Research, and Intezer. The NCFTA is an alliance of business and law enforcement working together to disrupt cybercrime.

The case was prosecuted by AUSA Jonathan Gottfried of the United States Attorney's Office for the District of Puerto Rico and Senior Counsel Jane Lee and Jeff Pearlman of the Department of Justice's Computer Crime and Intellectual Property Section, with assistance from the Office of International Affairs.

###

Updated November 14, 2023

Topic

Cybercrime