# Botnet Dismantled in International Operation, Russian and Kazakhstani Administrators Indicted

Published: 2025-05-09 · Archived: 2026-04-02 10:57:57 UTC

TULSA, Okla. – A domain seizure warrant was unsealed, along with an indictment charging four foreign national hackers with conspiracy and other computer crimes, announced U.S. Attorney Clint Johnson.

Russian nationals, Alexey Viktorovich Chertkov, 37, Kirill Vladimirovich Morozov, 41, Aleksandr Aleksandrovich Shishkin, 36, and Dmitriy Rubtsov, 38, a Kazakhstani national, were charged with *Conspiracy* and *Damage to Protected Computers* for conspiring with others to maintain, operate, and profit from botnet services known as Anyproxy and 5socks.

The Indictment alleges that a botnet was created by infecting older-model wireless internet routers worldwide, including in the United States, using malware without their owners' knowledge. The installed malware allowed the routers to be reconfigured, granting unauthorized access to third parties and making the routers available for sale as proxy servers on the Anyproxy.net and 5socks.net websites. Both website domains were managed by a company headquartered in Virginia and hosted on computer servers worldwide.

Additional court documents reveal that the 5socks.net website advertised more than 7,000 proxies for sale worldwide, including in the United States. Users paid a monthly subscription fee, ranging from $9.95 to $110 per month. The website's slogan, "Working since 2004!", indicates that the service has been available for more than 20 years. The defendants are believed to have amassed more than $46 million from selling access to the infected routers that were part of the Anyproxy botnet.

Chertkov and Rubtsov are additionally charged with *False Registration of a Domain Name.* They allegedly falsely identified themselves when they registered and used the domains Anyproxy.net and 5socks.net during the commission of these
felony crimes.

During the investigation, the FBI's Oklahoma City Cyber Task Force discovered that business and residential routers in Oklahoma had malware installed without the users' knowledge.

Pursuant to a seizure warrant in the Eastern District of Virginia and in conjunction with the unsealing of the Indictment in the Northern District of Oklahoma, the FBI seized the Anyproxy.net and 5socks.net domain names. The botnet overseas was also seized and disabled by foreign law enforcement partners.

The FBI Oklahoma City Cyber Task Force is investigating the case.

Assistant U.S. Attorneys George Jiang and Christopher J. Nassar, with the Northern District of Oklahoma, are prosecuting the case, along with Ryan K.J. Dickey and Jane Lee, Senior Counsel from the Computer Crime and Intellectual Property Section.

The Justice Department collaborated closely with investigators and prosecutors from multiple jurisdictions in this investigation, including the Eastern District of Virginia, the Dutch National Police – Amsterdam Region, the Netherlands Public Prosecution Service (Openbaar Ministerie), and the Royal Thai Police. Black Lotus Labs of Lumen Technologies, Inc., provided significant assistance and worked closely with investigators.

*An indictment is merely an allegation, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.*

---

## Victim Assistance Advisory for Owners of Wireless Internet Routers Infected by the Anyproxy/5socks Malware

On July 23, 2025, the U.S. District Judge John D. Russell issued an order directing the government to provide notice to potential victims in the United States v. Alexey Viktorovich Chertkov, et al., criminal case number, 25-CR-160.

In May 2025, an Indictment was unsealed charging four foreign national hackers for conspiring with others to maintain, operate, and profit from botnet services known as Anyproxy and 5socks. The Indictment alleges that a botnet was created by infecting older-model wireless internet routers worldwide, including in the United States, using malware without their owners' knowledge.

The installed malware allowed the routers to be reconfigured, granting unauthorized access to third parties and making the routers available for sale as proxy servers on the Anyproxy.net and 5socks.net websites. As part of the investigation, the FBI executed a federal search warrant directed at the infected devices located in the United States and further remediated the security vulnerabilities in 547 of them.

Members of the community who believe they may be the victim of this botnet may contact Victim Witness Coordinator and Supervisor, Brandi Duvall at 918-382-2700. For more information regarding the malware, please see Alert Number I-050725-PSA and FLASH-20250507-001 listed on the Internet Crime Complaint Center.

Court Documents

---