SEALED

FILED

MAY 05 2025

Heidi D. Campbell, Clerk
U.S. DISTRICT COURT

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA

UNITED STATES OF AMERICA,

Plaintiff,

v.

ALEXEY VIKTOROVICH CHERTKOV,
a/k/a "Mag,"
a/k/a "Andrey Romanocvich,"
a/k/a "Afanasiev Anton,"
KIRILL VLADIMIROVICH MOROZOV,
a/k/a "l0rda,"
DMITRIY RUBTSOV,
a/k/a "Vladimir Belyankin,"
ALEKSANDR ALEKSANDROVICH SHISHKIN,
a/k/a "SpekterX,"

Defendants.

Case No. 25 CR - 160 JDR

FILED UNDER SEAL

INDICTMENT

[COUNT ONE: 18 U.S.C. § 371 – Conspiracy;
COUNT TWO: 18 U.S.C. §§ 1030(a)(5)(A), 1030(c)(4)(B)(i), and 1030(c)(4)(A)(i)(VI) – Damage to Protected Computers;
COUNTS THREE and FOUR: 18 U.S.C. § 3559(g)(1) – False Registration of a Domain Name;
Forfeiture Allegation: 18 U.S.C. §§ 981(a)(1)(C), 982(a)(2)(B), 982(b)(1), 1030(i) and (j), 21 U.S.C. § 853(f) and (l), and 28 U.S.C. § 2461(c) – Conspiracy and Computer Crimes Forfeiture]

THE GRAND JURY CHARGES:

1. The defendants, **ALEXEY VIKTOROVICH CHERTKOV** (Алексей Викторович Чертков), a/k/a "Mag," a/k/a "Andrey Romanocvich," a/k/a "Afanasiev Anton," **KIRILL VLADIMIROVICH MOROZOV** (Кирилл Владимирович Морозов), a/k/a "l0rda," **DMITRIY RUBTSOV** (Дмитрий Рубцов), a/k/a "Vladimir Belyankin," and **ALEKSANDR ALEKSANDROVICH SHISHKIN** (Александр Александрович Шишкин), a/k/a "SpekterX," resided outside of the United States.

COUNT ONE
[18 U.S.C. § 371]

2. From as late as February 11, 2020, and continuing to on or about the date of this Indictment, in the Northern District of Oklahoma and elsewhere, the defendants, **ALEXEY VIKTOROVICH CHERTKOV**, a/k/a "Mag," a/k/a "Andrey Romanocvich," a/k/a "Afanasiev Anton," **KIRILL VLADIMIROVICH MOROZOV**, a/k/a "l0rda," **DMITRIY RUBTSOV**, a/k/a "Vladimir Belyankin," and **ALEKSANDR ALEKSANDROVICH SHISHKIN**, a/k/a "SpekterX," knowingly and intentionally combined, conspired, confederated, and agreed with each other and with other persons, both known and unknown to the Grand Jury, to commit offenses against the United States, in violation of Title 18, United States Code, Section 371, as follows:

PURPOSE OF THE CONSPIRACY

3. The purpose of the conspiracy was for the defendants to enrich themselves by selling to others backdoor access to compromised wireless internet routers for use as proxy servers.

OBJECT OF THE CONSPIRACY

4. The object of the conspiracy was to knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally cause damage without authorization to a protected computer, and the offense caused damage affecting 10 or more protected computers during a one-year period in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(B)(i), and 1030(c)(4)(A)(i)(VI).

MANNER AND MEANS OF THE CONSPIRACY

5. The conspiracy was to be accomplished, and was accomplished, by the following manner and means:

a. Conspirators maintained and operated a botnet (the Anyproxy botnet), which is a group of compromised computers connected in a coordinated fashion.

b. In order to operate the Anyproxy botnet, conspirators targeted popular older-model wireless internet routers, such as the Cisco Linksys E1200, that were exposed to known cybersecurity vulnerabilities in its remote access connection protocols. These wireless internet routers were connected to and could communicate over the internet. Because they

were connected to the internet, these devices were assigned Internet Protocol ("IP") addresses. An IP address is the unique series of numbers assigned to all computing devices connected to the internet.

c. Conspirators: (i) identified vulnerable wireless routers; (ii) gained unauthorized access to those devices using known cybersecurity vulnerabilities; (iii) installed malicious code on the routers; (iv) maintained a persistent connection even after the malicious code was cleared from memory; and (v) configured the compromised devices to grant unauthorized access to other actors. In this way, conspirators compromised thousands of wireless routers in the Northern District of Oklahoma and throughout the world and added them into the Anyproxy botnet without the authorization or knowledge of the owners of the devices.

d. Using the Anyproxy.net website, conspirators offered access to the Anyproxy botnet to others acting as re-sellers, such as 5socks.

e. Conspirators maintained and operated several computer servers in the Kingdom of the Netherlands, the Republic of Türkiye, and other locations to manage and maintain control over the Anyproxy botnet and operate the Anyproxy.net and 5socks.net websites.

f. Conspirators used JCS Fedora Communications ("Fedora"), a Russian internet hosting provider, to register and host servers used to operate the Anyproxy.net and 5socks.net websites.

g. Conspirators acting through 5socks offered access to the Anyproxy botnet for a monthly subscription fee at the online storefront 5socks.net. Customers of 5socks could either purchase a preset number of proxies that expire daily or a preset number of proxies that expire monthly to route their internet traffic through the compromised routers that had been enlisted into the botnet. In this way, the botnet subscribers' internet traffic appeared to come from the IP addresses assigned to the compromised devices rather than the IP addresses assigned to the devices that the subscribers were actually using to conduct their online activity.

h. Conspirators acting through 5socks publicly marketed the Anyproxy botnet as a residential[1] proxy service on social media and online discussion forums, including cybercriminal forums. Such residential proxy services are particularly useful to criminal hackers to provide anonymity when committing cybercrimes; residential—as opposed to commercial—IP addresses are generally assumed by internet security services as much more likely to be legitimate traffic. In this way, conspirators obtained a private financial gain from the sale of access to the compromised routers.

---

[1] The term "residential" was used by these services to convey to potential customers that the services being offered were not data-center proxies but were individuals or businesses, which can lead to greater anonymity for the customer.

OVERT ACTS

6. In furtherance of this conspiracy and to effect the objects thereof, the defendants, **CHERTKOV**, **MOROZOV**, **RUBTSOV**, and **SHISHKIN** committed the following overt acts, among others, in the Northern District of Oklahoma and elsewhere:

7. On or about November 9, 2004, **CHERTKOV** registered the domain Anyproxy.net, which hosts the website advertising the Anyproxy botnet proxies for sale and re-sale.

8. From as late as on or about March 5, 2005, to on or about the date of this Indictment, **CHERTKOV** served as the point of contact on Anyproxy.net website.

9. On or about September 13, 2006, **SHISHKIN** posted an advertisement for 5socks.net, which hosts an Anyproxy botnet storefront, on a website frequented by cybercriminals.

10. On or about March 17, 2007, **CHERTKOV** updated the registration for the domain 5socks.net.

11. On or about April 10, 2008, **RUBTSOV** updated the registration for the domain 5socks.net.

12. From on or about May 25, 2008 to on or about November 5, 2015, a member of the conspiracy unknown to the Grand Jury caused Anyproxy.net to use the name servers ns1.zon3.org and ns2.zon3.org, which were hosted by Fedora.

13. On or about June 28, 2008, **RUBTSOV** caused 5socks.net to use the name servers ns1.zon3.org and ns2.zon3.org, which were hosted by Fedora.

14. On or about September 21, 2008, **CHERTKOV** acted through Fedora to register the domain Anyproxy.net.

15. On or about September 19, 2011, **MOROZOV** acted through Fedora to register the domain zon3.org.

16. From as late as on or about September 2, 2011, to on or about the date of this Indictment, **RUBTSOV** served as the point of contact on the 5socks.net website.

17. Between on or about November 5, 2015 and May 11, 2016, **MOROZOV** caused Anyproxy.net to change the name servers to another service provider and continued to use this service provider for domain name services for Anyproxy.net to on or about the date of this Indictment.

18. On or about January 30, 2015, **RUBTSOV** caused 5socks.net to change the name servers to another service provider.

19. On or about February 19, 2015, **RUBTSOV** posted an advertisement for 5socks.net on a website frequented by cybercriminals.

20. On or about June 6, 2016, **RUBTSOV** updated the registration for the domain 5socks.net to reserve that domain until August 12, 2025.

21. From on or about September 24, 2018, to at least on or about March 6, 2020, **RUBTSOV** and **SHISHKIN** coordinated the administration and maintenance of

5socks.net, including handling customer service requests, collecting website usage metrics, and accounting for cryptocurrency payments by customers of the service.

22. As late as in or around April 2024, **RUBTSOV** and **CHERTKOV** coordinated for the payment of server hosting fees associated with Anyproxy.net.

23. On or about August 13, 2024, **CHERTKOV** updated the registration for the domain Anyproxy.net to reserve that domain until August 15, 2026.

24. On or about September 23, 2024, a member of the conspiracy unknown to the Grand Jury caused the 5socks.net website to sell access to a compromised Cisco Linksys E1200 wireless router located in the Northern District of Oklahoma that was part of the Anyproxy botnet for use as a proxy server without the authorization of the wireless router's owner.

All in violation of Title 18, United States Code, Section 371.

COUNT TWO
[18 U.S.C. §§ 1030(a)(5)(A), 1030(c)(4)(B)(i), and 1030(c)(4)(A)(i)(VI)]

25. The allegations in paragraphs 3 through 24 of this Indictment are incorporated by reference as if fully set forth herein.

26. On or about September 23, 2024, in the Northern District of Oklahoma and elsewhere, the defendants, **ALEXEY VIKTOROVICH CHERTKOV**, a/k/a "Mag," a/k/a "Andrey Romanocvich," a/k/a "Afanasiev Anton," **KIRILL VLADIMIROVICH MOROZOV**, a/k/a "l0rda," **DMITRIY RUBTSOV**, a/k/a "Vladimir Belyankin," and **ALEKSANDR ALEKSANDROVICH SHISHKIN**, a/k/a "SpekterX," aiding and abetting each other and others known and unknown to the Grand Jury, knowingly caused the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally caused damage without authorization to a protected computer, and the offense caused damage affecting 10 or more protected computers during a one-year period, specifically, the defendants and their accomplices modified the data storing the network settings of a protected computer in the Northern District of Oklahoma to enable the defendants and their accomplices to then sell access to that protected computer's system and network resources to others as part of the Anyproxy botnet, and did so to nine or more other protected computers elsewhere during the one-year period ending on or about the date of this Indictment.

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A), (c)(4)(B)(i), and (c)(4)(A)(i)(VI).

COUNT THREE
[18 U.S.C. § 3559(g)(1)]

27. The allegations in paragraphs 3 through 24 of this Indictment are incorporated by reference as if fully set forth herein.

28. From as late as on or about August 13, 2024, and continuing to on or about the date of this Indictment, in the Northern District of Oklahoma and elsewhere, **ALEXEY VIKTOROVICH CHERTKOV**, a/k/a "Mag," a/k/a "Andrey Romanocvich," a/k/a "Afanasiev Anton," knowingly falsely registered and caused to be registered the Anyproxy.net domain name and used that domain name in the course of the offenses described in Counts One and Two of this Indictment.

All in violation of Title 18, United States Code, Section 3559(g)(1).

COUNT FOUR
[18 U.S.C. § 3559(g)(1)]

29. The allegations in paragraphs 3 through 24 of this Indictment are incorporated by reference as if fully set forth herein.

30. From as late as on or about September 23, 2024, and continuing to on or about the date of this Indictment, in the Northern District of Oklahoma and elsewhere, **DMITRIY RUBTSOV**, a/k/a "Vladimir Belyankin," knowingly falsely registered and caused to be registered the 5socks.net domain name and used that domain name in the course of the offenses described in Counts One and Two of this Indictment.

All in violation of Title 18, United States Code, Section 3559(g)(1).

FORFEITURE ALLEGATION
[18 U.S.C. § 981(a)(1)(C), 982(a)(2)(B), 982(b)(1), 1030(i) and (j), 21 U.S.C. § 853(f) and (l), and 28 U.S.C. § 2461(c)]

The allegations contained in this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeitures pursuant to Title 18, United States Code, Sections 981(a)(1)(C), 982(a)(2)(B), 1030(i) and (j), Title 21, United States Code, Sections 853(f) and (l), and Title 28, United States Code, Section 2461(c).

Upon conviction of the offenses alleged in this Indictment, as a part of his sentence, the defendants, **ALEXEY VIKTOROVICH CHERTKOV**, a/k/a "Mag," a/k/a "Andrey Romanocvich," a/k/a "Afanasiev Anton," **KIRILL VLADIMIROVICH MOROZOV**, a/k/a "l0rda," **DMITRIY RUBTSOV**, a/k/a "Vladimir Belyankin," and **ALEKSANDR ALEKSANDROVICH SHISHKIN**, a/k/a "SpekterX," shall forfeit to the United States any property constituting, or derived from, or traceable to, the proceeds obtained, directly or indirectly, as a result of such violations and any property, real or personal, that was used or intended to be used to commit or to facilitate the violations of federal law. The property to be forfeited includes, but is not limited to:

DOMAIN NAMES

1. Anyproxy.net;
2. 5socks.net; and

MONEY JUDGMENT

3. A money judgment in an amount of at least $46,541,629.05, representing proceeds obtained by the defendants as a result of the offenses.

Pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 982(b)(1) and 1028(g), and Title 28, United States Code, Section 2461(c), the defendant shall forfeit substitute property, up to the value of the property described above if, by any act or omission of the defendant, the property described above, or any portion thereof, cannot be located upon the exercise of due diligence; has been transferred or sold to, or deposited with, a third party; has been placed beyond the jurisdiction of the court; has been substantially diminished in value; or has been commingled with other property which cannot be divided without difficulty.

All pursuant to Title 18, United States Code, Sections 981(a)(1)(C), 982(a)(2)(B), 1030(i) and (j), Title 21, United States Code, Sections 853(f) and (l), and Title 28, United States Code, Section 2461(c).

CLINTON J. JOHNSON
United States Attorney

A TRUE BILL

GEORGE JIANG
Assistant United States Attorney

/s/ Grand Jury Foreperson
Grand Jury Foreperson

RYAN K.J. DICKEY
JANE LEE
Senior Counsel
Computer Crime and Intellectual Property Section
Criminal Division, U.S. Department of Justice