UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

October 2024 Grand Jury

UNITED STATES OF AMERICA,

Plaintiff,

v.

VICTORIA EDUARDOVNA DUBRANOVA,
aka "Vika,"
aka "Tory,"
aka "Sovasonya,"
[redacted]

2:25-578(A)-SRM

I N D I C T M E N T

[18 U.S.C. § 371: Conspiracy; 18 U.S.C. § 1030: Criminal Forfeiture]

[redacted]

Defendants.

The Grand Jury charges:

[18 U.S.C. § 371]

[ALL DEFENDANTS]

A. INTRODUCTORY ALLEGATIONS & DEFINITIONS

At all times relevant to this Indictment:

The Conspiracy and Defendants

1. NoName057(16) (also known as "NoName" and "Noname057") was a group that conducted cyberattacks, including distributed denial of service attacks, or "DDoS," against critical infrastructure and other victims around the world, in support of Russia's geopolitical interests.

2. The Center for the Study and Network Monitoring of the Youth Environment ("CISM") (in Cyrillic, "Центр изучения и сетевого мониторинга молодёжной среды," abbreviated to "Цисм"), was an information technology organization established by order of the President of Russia in October 2018 that purported to, among other things, monitor the safety of the internet for Russian youth. CISM undertook overt projects, such a studying risks to youth safety online, as well as covert projects, like administrating and

coordinating NoName057(16)'s cybercampaign.

3. Defendants VICTORIA EDUARDOVNA DUBRANOVA, also known as ("aka") "Vika," aka "Tory," aka "Sovasonya," ("DUBRANOVA"); [redacted] were members of NoName057(16).

4. [redacted]

5. [redacted]

6. Defendants [redacted] and [redacted] were employees of CISM.

7. All defendants, except defendant DUBRANOVA, were residents of Russia. Defendant DUBRANOVA was a resident of Ukraine.

8. At times, NoName057(16)'s Telegram public channels collectively had between 10,000 and 52,000 followers, including followers in the United States.

Definitions

9. A DDoS attack is a type of computer-based attack in which an internet-connected victim computer is flooded with data and/or queries in such a manner to render it unable to communicate with other devices on the Internet or to perform the services which it is intended to perform.

10. Telegram is a cloud-based encrypted messaging service that allows users to post messages in public channels and message other users directly.

11. GitHub is a host of software repositories, both open source and private, using the Git version control system. The primary purpose of this system is to allow large teams of coders to edit each other's submissions in a controlled and well-organized fashion. The information contained in these repositories can include the code itself, previous versions of the code, information about collaborators, contributors and repository members, logs of Git operations, and other information about the project and network of contributors.

B. OBJECTS OF THE CONSPIRACY

Beginning no later than March 2022, and continuing to the present, in Los Angeles County, within the Central District of California, and elsewhere, defendants DUBRANOVA, [redacted], and others known and unknown to the Grand Jury, knowingly conspired and agreed with each other to knowingly cause the transmission of programs, information, codes, and commands, and as a result of such conduct, intentionally cause damage without authorization to protected computers, and specifically:

a. to cause loss to one or more persons during a one-year period, and resulting from a related course of conduct affecting one or more protected computers, aggregating at least $5,000 in value, in violation of Title 18, United States Code, Section 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I); and

b. to cause damage affecting ten or more protected computers during a one-year period, in violation of Title 18, United States Code, Section 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(VI).

C. MEANS BY WHICH THE OBJECTS OF THE CONSPIRACY WERE TO BE ACCOMPLISHED

The objects of the conspiracy were to be accomplished, in substance, as follows:

1. Defendants [redacted] and [redacted] who were CISM employees, defendant [redacted] and co-conspirators would develop and customize NoName057(16)'s proprietary DDoS program, DDoSia, using GitHub and other types of software repository project management systems;

2. Using cryptocurrency payments, defendant [redacted] and co-conspirators would pay hosting companies around the world that hosted servers used for NoName057(16)'s network infrastructure;

3. Co-conspirators would use Virtual Private Networks ("VPNs"), including a VPN with servers in the Central District of California, to conduct cyberattacks.

4. Defendants [redacted] and [redacted] would monitor co-conspirators, who would research and identify potential victims for NoName057(16) cyberattacks, including by probing for network vulnerabilities and examining potential websites for future attacks;

5. Using private Telegram chats and other means of

communication, defendants, including defendant [redacted] would coordinate cyberattacks against victims around the world, including victims allied with the United States;

6. Defendants [redacted] [redacted] DUBRANOVA, and co-conspirators would serve as administrators for various private Telegram chats and public Telegram channels associated with NoName057(16), including English- and Russian-language Telegram channels, controlling the membership in the chats and moderating posts in the channels;

7. Defendant [redacted] would serve as a moderator of the public Telegram channels associated with NoName057(16), and moderating posts and access privileges in the channels;

8. Defendant [redacted] and other co-conspirators from around the world would affirm they had read the NoName057(16) "Manifesto" in order to join NoName057(16)'s public Telegram channels;

9. Defendant [redacted] and co-conspirators would instruct NoName057(16) members in the public Telegram channels on how to download the DDoSia script from a GitHub repository onto their own computers;

10. Co-conspirators would post a list of targets on the Telegram channels for followers to launch coordinated DDoS attacks using DDoSia against hundreds of victims around the world, including websites of government institutions, financial institutions, and critical infrastructure;

11. Co-conspirators would post on the public NoName057(16) Telegram channels purported explanations for why NoName057(16) had targeted those victims, including in support of Russian geopolitical interests;

12. NoName057(16) members, including defendant [redacted] would launch multiple DDoS attacks against the chosen targets from their own computers around the world;

13. NoName057(16) would publish a daily leaderboard of volunteers who launched the most DDoS attacks on its Telegram channel;

14. NoName057(16) would pay the top-ranking members in cryptocurrency through a wallet server within the DDoSia infrastructure;

15. On NoName057(16)'s public Telegram channels, co-conspirators, including Telegram administrators, would post a link to a network monitoring tool that indicated that the DDoS victim website had been taken offline (i.e., that the cyberattack was successful);

16. Defendants [redacted] [redacted] and co-conspirators would search the internet for press coverage of NoName057(16)'s DDoSia attacks in the days and weeks that followed the attacks to gauge their impact and notoriety.

17. Defendant [redacted] and co-conspirators would use web-based tools to monitor NoName057(16)'s Telegram presence and user engagement.

18. Defendant [redacted] and co-conspirators would share links to the DDoSia download page in the public Telegram channel and private Telegram messages to recruit new members to join NoName057(16).

19. Defendants [redacted] and DUBRANOVA, and co-conspirators, would create promotional media to increase NoName057(16)'s notoriety and recruit new members.

20. Co-conspirators would repost and promote the cyberattacks

by other hacktivist groups either formally or informally allied with NoName057(16).

D. OVERT ACTS

In furtherance of the conspiracy and to accomplish its objects, on or about the following dates, defendants DUBRANOVA, [redacted], and others, committed various overt acts within the Central District of California, and elsewhere, including but not limited to the following:

Development of DDoSia Malware

Overt Act No. 1: On an unknown date, defendant [redacted] edited the DDoSia programming code in a GitHub repository called "ddos_config."

Overt Act No. 2: On an unknown date, but no later than January 16, 2023, defendant [redacted] joined the NoName Telegram channel.

Overt Act No. 3: On January 16, 2023, defendant [redacted] edited the programming code for DDoSia in the DDoSia GitHub repository to add a "targets dropdown."

Overt Act No. 4: On January 25, 2023, defendant [redacted] edited the programming code for DDoSia in the DDoSia GitHub repository to add a domain checker function, which is a tool that checks the availability and security of a domain name and can be used to gauge the vulnerability to or success of a DDoS attack.

Overt Act No. 5: On February 17, 2023, defendant [redacted] edited the DDoSia programming code in a GitHub repository called "ddos_config."

Overt Act No. 6: On February 22, 2023, defendant [redacted]

edited the programming code in a GitHub repository for the backend administration of the DDoSia network called "dosia_administration."

Overt Act No. 7: On April 13, 2023, defendant [redacted] using an official CISM email address, directed defendant [redacted] to contact him about a job opening for a "web analyst" at CISM.

Overt Act No. 8: On an unknown date, but no earlier than June 28, 2023, defendant [redacted] joined CISM as a program developer.

Overt Act No. 9: On June 28, 2023, defendant [redacted] edited the DDoSia programming code in a GitHub repository called "ddos_config."

Overt Act No. 10: On October 6, 2023, defendant [redacted] edited the DDoSia programming code in a repository called "ddos_config" using a GitHub account registered a CISM email address.

Administration, Promotion, and Coordination of NoName

Overt Act No. 11: On July 7, 2022, defendant [redacted] joined one of NoName's Telegram bots.

Overt Act No. 12: Between no later than July 7, 2022 and June 8, 2024, defendant [redacted] logged into a server that NoName used to probe potential DDoSia targets, including websites for European Union and Polish critical infrastructure for vulnerabilities, at least 1,772 times.

Overt Act No. 13: On an unknown date, defendant [redacted] joined the NoName public Telegram channel.

Overt Act No. 14: On an unknown date, defendant [redacted] joined the NoName Telegram channel.

Overt Act No. 15: On December 28, 2022, defendant [redacted] sent 1.13762 Litecoin ("LTC"), a cryptocurrency, to a NoName cryptocurrency wallet used to pay a hosting service provider, which

hosted a known DDoSia command and control ("C2") server.

Overt Act No. 16: On February 10, 2023, defendant [redacted] sent 1.485451 LTC to a NoName cryptocurrency wallet used to pay a proxy hosting service that hosted NoName proxy servers.

Overt Act No. 17: On May 10, 2023, defendant [redacted] logged into the server that NoName used to probe potential DDoSia targets.

Overt Act No. 18: On July 26, 2023, defendant [redacted] searched the internet for information about the "DDosia project" and "noname057" on Wikipedia and a Russian hacker publication.

Overt Act No. 19: On August 7, 2023, defendant [redacted] sent 3.99737 LTC, to a NoName cryptocurrency wallet used to pay the hosting service provider which had previously hosted a DDoSia C2 server.

Overt Act No. 20: No later than May 9, 2024, defendant DUBRANOVA assisted in the creation of a NoName promotional video later posted to NoName's Telegram channels.

Overt Act No. 21: On August 26, 2024, defendant [redacted] in a private Telegram chat, shared a link with co-conspirators, including user "DDoSia Project," to an online document titled "Instructions on Security for the Volunteer Project DDoSia Project 7-22."

Overt Act No. 22: On August 26, 2024, defendant [redacted] searched the internet for information about Spain's arrest of NoName members, which occurred on July 20, 2024.

Overt Act No. 23: On September 11, 2024, in a private Telegram chat, defendant [redacted] circulated the NoName Telegram channel, introducing it as a "group for our volunteer project," DDoSia Project.

Overt Act No. 24: On September 11, 2024, in a private Telegram chat with defendant DUBRANOVA, defendant [redacted] shared a script directing DUBRANOVA to create an animated recruitment video showing that "anyone can become a volunteer for DDoSia Project."

Overt Act No. 25: On September 27, 2024, defendant [redacted] sent unknown co-conspirators via a private Telegram chat six Austrian websites to launch DDoS attacks against, explaining that "elections [w]ere coming in Austria" and "We want to rip them off." These targets included a bank and various railway websites.

Overt Act No. 26: Between approximately October 15, 2024, and November 3, 2024, defendant [redacted] participated in a private Telegram chat that included [redacted] discussing a "deserved[] ban" on a member that [redacted] imposed in his capacity as a moderator.

Overt Act No. 27: On October 31, 2024, defendant [redacted] in a private Telegram chat requested the cryptocurrency wallet for an unnamed co-conspirator to "send them a coin."

Overt Act No. 28: On December 10, 2024, defendant [redacted] logged into a project management web service to view a page called "NN+Shadow+personal."

Overt Act No. 29: On January 17, 2025, defendant [redacted] tracked NoName's Telegram presence, including the channel's profile analytics and statistics, through the tool TGStat.

Overt Act No. 30: On February 15, 2025, defendant [redacted] researched on the internet how to use the computer program, Nmap, to scan "all ports" of a computer network for open ports and/or vulnerabilities.

Overt Act No. 31: On an unknown date, but no later than April 8, 2025, defendant [redacted] possessed a GitHub repository for a DDoS

script called "DDoS-PHP-Script."

DDoS Targeting and Attacks

Overt Act No. 32: On June 12, 2023, co-conspirators launched DDoS attacks against several Swiss governmental websites and interrupted their services.

Overt Act No. 33: On July 7, 2023, a co-conspirator claimed credit for DDoS attacks against various Polish websites, including the website for a railway management company, in the public NoName Telegram channel.

Overt Act No. 34: On a date unknown, defendant [redacted] joined the NoName057(16) Telegram channel.

Overt Act No. 35: On May 21 and 22, 2024, defendant [redacted] operated infrastructure that was the source of the highest DDoS attack load against at least multiple German victim websites.

Overt Act No. 36: On June 14, 2024, defendant [redacted] ordered VPS services which he used to launch DDoSia attacks.

Overt Act No. 37: On June 19, 2024, defendant [redacted] ordered VPS services which he used to launch DDoSia attacks.

Overt Act No. 38: On August 21, 2024, defendant [redacted] provided an individual from the NoName Telegram channel with a copy of DDoSia.

Overt Act No. 39: On August 21, 2024, defendant [redacted] instructed the individual how to run DDoSia, and the individual successfully completed a DDoS attack against a Latvian victim website.

Overt Act No. 40: On September 18, 2024, co-conspirators launched DDoSia attacks against various Austrian victims, including financial institutions.

Overt Act No. 41: On September 25, 2024, a co-conspirator posted in the public NoName Telegram channel, "We continue sending DDoS-missiles to the sites of critical infrastructure in Austria 😈," claiming credit for several days of cyber attacks against Austrian municipalities and governmental institutions, among other victims, ahead of the September 29, 2024 Austrian parliamentary election.

Overt Act No. 42: On October 7, 2024, a co-conspirator posted in the public NoName Telegram channel that "We have decided to pay a visit to Russophobic Belgium to show them how initiatives in support of the criminal regime in Kyiv end."

Overt Act No. 43: On October 8, 2024, a co-conspirator posted a list of Belgian municipalities and ports to target for DDoS attacks, including the websites of the ports of two port cities, approximately one week before Belgian local elections.

Overt Act No. 44: On October 10, 2024, a co-conspirator posted on the NoName public Telegram channel "Check Host" links to numerous Belgian websites, including those of the targeted ports publicized on October 8, 2024, showing that those websites, were, in fact, attacked between October 7 and 10, 2024.

Overt Act No. 45: On June 23, 2025, a NoName co-conspirator claimed credit for DDoS attacks against 10 Dutch victims ahead of the 2025 North Atlantic Treaty Organization ("NATO") Summit at the Hague.

Overt Act No. 46: On June 25, 2025, the second day of the NATO Summit, a NoName co-conspirator claimed credit for DDoS attacks against several Dutch transportation organizations.

FORFEITURE ALLEGATION

[18 U.S.C. § 1030]

1. Pursuant to Rule 32.2(a) of the Federal Rules of Criminal Procedure, notice is hereby given that the United States will seek forfeiture as part of any sentence, pursuant to Title 18, United States Code 1030, in the event any defendant's conviction of the offense set forth in this Indictment.

2. Any defendant so convicted shall forfeit to the United States of America the following:

a. All right, title, and interest in any and all property, real or personal, constituting, or derived from, any proceeds obtained, directly or indirectly, as a result of the offense;

b. Any property used or intended to be used to commit the offense; and

c. To the extent such property is not available for forfeiture, a sum of money equal to the total value of the property described in subparagraphs (a) and (b).

3. Pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code 1030(i), any defendant so convicted shall forfeit substitute property, up to the total value of the property described in the preceding paragraph if, as the result of any act or omission of said defendant, the property described in the preceding paragraph, or any portion thereof: (a) cannot be located upon the exercise of due diligence;

//

//

//

(b) has been transferred, sold to or deposited with a third party; (c) has been placed beyond the jurisdiction of the court; (d) has been substantially diminished in value; or (e) has been commingled with other property that cannot be divided without difficulty.

A TRUE BILL

/S/
Foreperson

BILAL A. ESSAYLI
United States Attorney

DAVID T. RYAN
Assistant United States Attorney
Chief, National Security Division

IAN V. YANNIELLO
Assistant United States Attorney
Chief, Terrorism & Export Crimes Section

ANGELA C. MAKABALI
Assistant United States Attorney
Terrorism & Export Crimes Section

ALEXANDER S. GORIN
Assistant United States Attorney
Terrorism & Export Crimes Section