

KOG/240807
ASJZ/RIG USAO 2022R00237

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

SDC - BALTIMORE
24 AUG 7 AM 11:55

UNITED STATES OF AMERICA

v.

AMIN STIGAL,
VLADISLAV BOROVKOV,
DENIS DENISENKO,
YURIY DENISOV,
DMITRIY GOLOSHUBOV, and
NIKOLAY KORCHAGIN

Defendants.

FILED UNDER SEAL

CRIMINAL NO. LKG-24-206

(Conspiracy to Commit Computer Intrusion
and Damage (18 U.S.C. § 371); Wire Fraud
Conspiracy (18 U.S.C. § 1349); Forfeiture (18
U.S.C. §§ 981, 982, and 1030(i), 21 U.S.C. §
853(p)), and 28 U.S.C. § 2461(c))

SUPERSEDING INDICTMENT

COUNT 1

(Conspiracy to Commit Fraud and Related Activity in Connection with Computers)

The Grand Jury for the District of Maryland charges that:

At all times relevant:

1. The Russian Federation (“Russia”) operated a military intelligence agency called the Main Intelligence Directorate of the General Staff (“GRU”). Within the GRU, Military Unit 29155 engaged in cyber operations that, among other things, involved the destruction of computer systems in foreign countries through computer intrusions. From in or around December 2020 to the present, Unit 29155 conducted large-scale cyber operations to harm computer systems in Ukraine prior to the 2022 Russian invasion. Beginning in or about August 2021, Unit 29155 also probed a variety of protected computer systems including those associated with twenty-six NATO member countries, searching for potential vulnerabilities. In or about October 2022, Unit 29155 also gained access to protected computers associated with the transportation sector in a Central European country (“Central European Country 1”).

2. Defendants **VLADISLAV BOROVKOV, DENIS DENISENKO, YURIY DENISOV, DMITRIY GOLOSHUBOV,** and **NIKOLAY KORCHAGIN** were GRU officers and members of Unit 29155 who knowingly conspired with **AMIN STIGAL**, a Russian citizen and civilian, and others known and unknown to the Grand Jury, (collectively the “Conspirators”), to gain unauthorized access (to “hack”) into computers associated with the Ukrainian Government and entities associated with the governments of countries that provided support to the Ukrainian Government in resisting Russia’s invasion of Ukraine.

3. First, in the month prior to the full-scale Russian invasion of Ukraine in February 2022, the Conspirators hacked the computers of dozens of Ukrainian Government entities and destroyed or attempted to destroy those computers in advance of the Russian invasion of Ukraine. They attacked computers involved in critical infrastructure, as well as entities responsible for other sectors with no military or defense-related roles, including agriculture, education and science, and emergency services. The Conspirators used software that was designed to appear as if the computers had suffered a ransomware attack, when in fact the data on the computers had been deleted. The Conspirators also stole and leaked through online platforms the personal data of thousands of Ukrainian civilians, including medical records. The purpose of the attack was, in part, to sow concern among Ukrainian citizens regarding the safety of their government’s systems and their personal data in advance of the Russian attack of Ukraine. This campaign became publicly known in cybersecurity circles as the “WhisperGate” campaign.

4. In addition, from August 2021 through at least December 2022, the Conspirators probed computer systems in at least twenty-six NATO countries searching for vulnerabilities.

5. In October 2022, the Conspirators hacked Central European Country 1’s transportation infrastructure. Central European Country 1 was a supporter of Ukraine and had

delivered civilian and military aid to Ukraine following the Russian invasion of Ukraine in February 2022.

6. From August 2021 through at least February 2022, the Conspirators also probed systems in the United States, including multiple sites maintained by a U.S. Government Agency located in Maryland.

7. To conceal their connections to Russia and the Russian Government, the Conspirators used false identities and made false statements about their identities. To further avoid detection, the Conspirators used a network of computers located across the world, including in the United States, and paid for infrastructure and tools using cryptocurrency and electronic payments.

Defendants

8. Defendant **YURIY DENISOV** [Юрий Денисов] was a colonel in the Russian military and a commanding officer of cyber operations for Unit 29155. **DENISOV** is pictured below:



YURIY DENISOV

9. Defendant **VLADISLAV BOROVKOV** [Владислав Боровков], was a lieutenant in the Russian military assigned to Unit 29155 who worked on cyber operations.

10. Defendant **DENIS DENISENKO** [Денис Денисенко] was a lieutenant in the Russian military assigned to Unit 29155 who worked on cyber operations.

11. Defendant **DMITRIY GOLOSHUBOV** [Дима Голошубов] was a lieutenant in the Russian military assigned to Unit 29155 who worked on cyber operations.

12. Defendant **NIKOLAY KORCHAGIN** [Николай Корчагин] was a lieutenant in the Russian military assigned to Unit 29155 who worked on cyber operations.

13. Lieutenants **BOROVKOV, DENISENKO, GOLOSHUBOV,** and **KORCHAGIN** are pictured below:



14. Defendant **AMIN STIGAL** [Амин Стигал] was a Russian citizen who supported the activities of Unit 29155 by setting up online infrastructure for members of Unit 29155 to use

in cyberattacks, including in the deployment of the WhisperGate malware described further below.

STIGAL is pictured below:



AMIN STIGAL

15. Unit 29155 was responsible for hacking Ukrainian Government entities, including those involving critical infrastructure, as well as entities responsible for other sectors with no military or defense-related roles, including agriculture, education and science, and emergency services, and destroyed or attempted to destroy those systems in advance of the full-scale Russian invasion of Ukraine in February 2022.

Relevant Terms

16. “Bitcoin” or “BTC” was a type of virtual currency, circulated over the Internet as a form of value. Bitcoin were not issued by any Government, bank, or company, but rather were generated and controlled through computer software programs operating via a decentralized, peer-to-peer network. Bitcoin were just one of many varieties of virtual currency.

17. A “darknet website” was a hidden website available through a network of globally distributed relay computers called The Onion Router, or “Tor,” network. Unlike standard Internet websites, Tor-based websites anonymized Internet activity by routing a user’s communications through a global network of relay computers (or proxies), thus effectively masking information about the user’s computer.

18. “Encryption” was a way of scrambling data so that only authorized parties could read or understand the information. In order to access encrypted data, a user had to have access to a password (known as a “decryption key”) that enabled the user to decrypt it.

19. “Malware” was malicious computer software intended, when successfully installed, to cause the victim computer to behave in a manner inconsistent with the intention of the owner or user of the victim computer, usually unbeknownst to that person.

20. “Ransomware” was a form of malware that infected a computer and encrypted some or all of the data on the computer. Once data on a computer was encrypted, distributors of ransomware would extort victims by demanding a ransom in exchange for the decryption key needed to regain access to the encrypted data on the computer.

21. Voice Over Internet Protocol “VOIP” was a technology that allowed users to make voice calls using a broadband Internet connection instead of a regular phone line.

The Conspiracy

22. Beginning no later than in or around December, 2020, and continuing through the date of this Superseding Indictment, in an offense that began outside the jurisdiction of any particular State or district of the United States, and continued in the District of Maryland and elsewhere, the defendants, **AMIN STIGAL, VLADISLAV BOROVKOV, DENIS DENISENKO, YURIY DENISOV, DMITRIY GOLOSHUBOV,** and **NIKOLAY**

KORCHAGIN, did knowingly and unlawfully conspire with each other and with others known and unknown to the Grand Jury to commit an offense against the United States, that is:

- a. 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, with such offense causing: loss to 1 or more persons during a 1-year period aggregating at least \$5,000 in value; and damage affecting 10 or more protected computers during a 1-year period; in violation of Title 18, United States Code, Section 1030(a)(5)(A) and (c)(4)(B).

Object of the Conspiracy

23. The object of the conspiracy was for the Conspirators to identify and exploit vulnerabilities in, and obtain unauthorized access to, protected computers belonging to target Governments and infrastructure systems outside of Russia in order to cause damage and render the targeted protected computers inoperable. It was a further object of the conspiracy for the Conspirators to exfiltrate data from protected computers and stage public releases of that data in order to embarrass a target Government and create concern among its citizens about vulnerabilities to cyberattack.

Manner and Means of the Conspiracy

24. From December 2020 through the date of this Superseding Indictment, the Conspirators scanned protected computers worldwide, including in the District of Maryland, for possible vulnerabilities as a preliminary step toward gaining unauthorized access to those protected computers.

25. It was further part of the conspiracy that the Conspirators gained unauthorized access to protected computers by exploiting those vulnerabilities identified through the scanning and then stole copies of files and programs they accessed from the targeted protected computers.

26. It was further part of the conspiracy that the Conspirators would infect protected computers with malware, which would render those computers unusable. The malware was disguised to appear like ransomware, but in fact would leave the victims with no method to recover their data.

27. It was further part of the conspiracy that the Conspirators would exfiltrate data from the targeted protected computers prior to disabling them, and would post that data, including personal information of individuals, for sale on the Internet. The data was posted, in part, to sow concern among Ukrainian citizens regarding the safety and security of their government's systems and their personal data in advance of the Russian invasion of Ukraine.

Overt Acts

Unit 29155 Searches Worldwide Computers for Vulnerabilities

28. The Conspirators identified potential victims by first scanning the potential victims' computer systems for vulnerabilities that the Conspirators could exploit to gain access. Beginning by at least August 2021, the Conspirators scanned computer systems in Ukraine and the computer systems of at least twenty-six NATO countries for vulnerabilities, including but not limited to:

a. Beginning in August 2021 and continuing through October 2021, the Conspirators scanned more than 2,400 public-facing Ukrainian Government websites for potential vulnerabilities, including Diia.gov.ua (DIIA), the website for a Ukrainian Government application that was built in partnership with the United States and allowed the Ukrainian people to connect with Ukrainian Government services and access Ukrainian

Government documents, as well as the websites associated with various cities in Ukraine, and the Ukrainian Government, including Ukrainian Ministry of Internal Affairs, the State Treasury, the Judiciary Administration, the State Portal for Digital Services, the Ministry of Education and Science, the Ministry of Agriculture, the State Service for Food Safety and Consumer Protection, the Ministry of Energy, the Accounting Chamber for Ukraine, the State Emergency Service, the State Forestry Agency, and the Motor Insurance Bureau.

b. In January 2022, the Conspirators probed a variety of protected computer systems associated with the Ukrainian Government for potential vulnerabilities, including the State Treasury of Ukraine, Ukrainian Maritime Services, and Ukrainian Railways.

c. On or about November 15, 2022, the Conspirators scanned a domain associated with a Central European country (“Central European Country 2”).

d. On or about November 16, 2022, the Conspirators scanned 270 domains associated with kitsoft.kiev.ua. KitSoft was a Ukrainian webhosting company.

e. On or about November 17, 2022, the Conspirators scanned at least 130 domains associated with the embassies of a foreign country.

f. On or about November 18, 2022, the Conspirators scanned a domain associated with Central European Country 1’s transportation sector at least 68 times.

g. On or about December 4, 2022, the Conspirators scanned a domain associated with a Central European country (“Central European Country 3”).

h. On or about December 12, 2022, the Conspirators scanned a domain associated with a Western European country.

STIGAL Creates Conspirators' Accounts

29. On or about December 2020, **STIGAL** created or caused to be created an account on Company 1's servers for the purpose of use in the Conspirators' attacks. Company 1 provided a messaging and VOIP platform and was located in the United States.

30. From on or about September 17, 2021, through on or about January 28, 2022, **STIGAL** created or caused to be created five accounts on Company 1's servers for the purpose of use in the Conspirators' attacks.

31. From on or about September 17, 2021, through on or about January 18, 2022, **STIGAL** and other Conspirators caused more than 225 files, including numerous malware scripts, to be uploaded to accounts on Company 1's servers, including to accounts controlled by **STIGAL**.

Testing of WhisperGate Malware

32. On or about January 10, 2022, several days prior to the WhisperGate attack on Ukraine, the Conspirators tested the efficacy of the WhisperGate malware.

Attack on Ukrainian Government Computer Systems

33. On or about January 13, 2022, the Conspirators attacked protected computers of at least two dozen Ukrainian Government networks, including the Ministry of Internal Affairs, the State Treasury, the Judiciary Administration, the State Portal for Digital Services (DIIA), the Ministry of Education and Science, the Ministry of Agriculture, the State Service for Food Safety and Consumer Protection, the Ministry of Energy, the Accounting Chamber for Ukraine, the State Emergency Service, the State Forestry Agency, and the Motor Insurance Bureau, using the malware program known as WhisperGate.

34. The Conspirators' attacks infected the targeted protected computers associated with the Ukrainian Government networks with WhisperGate, which uses a two-stage malware program.

The first stage wiped the Master Boot Record (“MBR”) from each targeted computer. The MBR allows an operating system to be loaded (booted) into a usable interface. Without an MBR, a computer is unable to restart or operate normally.

35. The Conspirators also caused a ransom note to be placed on each targeted protected computer stating:

Your hard drive has been corrupted. In case you want to recover all hard drives of your organization, You [sic] should pay us \$10k via bitcoin wallet [address] and send message . . . with your organization name. We will contact you to give further instructions.

In truth, as described further below, although a ransom note was displayed, the data on the targeted computers was destroyed, and therefore not recoverable even if a ransom were paid.

36. The Conspirators also caused the second stage of the malware to be activated. This stage contained a “GET” request to a URL maintained by Company 1. That request resulted in the downloading and execution of a program from an account on Company 1’s servers that the Conspirators had created. The program corrupted the files on the targeted protected computer, rendering the protected computer inoperable and entirely deleting data from the computer systems.

37. On or about that same date, January 13, 2022, the Conspirators compromised protected computers hosting the DIIA website and other websites, and caused a message to be displayed in Polish, Russian, and Ukrainian reading: “Ukrainians! All information about you has become public, be afraid and expect the worst. This is for your past, present and future.”

Release of Exfiltrated Information

38. Within hours of the attack, on or about January 13, 2022, the Conspirators listed for sale data described as originating from the Ukrainian Government on forums across the darknet, using the moniker “Free Civilian,” including:

- a. Criminal records obtained from Ukrainian Government systems;

- b. Patient health data from Ukrainian Government systems; and
- c. Motor Insurance Bureau information from Ukrainian Government systems.

39. On that same day, the Conspirators also offered for sale on the Internet data for 13.5 million users from Diia.gov.ua for \$80,000.

Central European Country 1 Infrastructure Attack

40. In October 2022, the Conspirators probed computer networks associated with Central European Country 1's transportation sector. Central European Country 1 was a supporter of Ukraine and had delivered civilian and military aid to Ukraine following the Russian invasion of Ukraine in February 2022.

41. As a result of the vulnerabilities the Conspirators discovered from their probing activities, they gained unauthorized access to protected computers associated with Central European Country 1's transportation sector in or around October 2022.

Scanning of U.S. Government Assets in Maryland

42. From on or about August 5, 2021, through on or about February 3, 2022, the Conspirators probed public-facing websites hosted by protected computers and unassigned servers maintained by a U.S. Government Agency located in Maryland, 63 times. This probing used the same servers that the Conspirators previously employed to conduct scanning against potential targets.

Meetings of Conspirators at Cafe Shokoladnitsa

43. In or about April and May 2023, the Conspirators, including **DENISOV**, **DENISKNO**, **KORCHAGIN**, **GOLOSHUBOV**, **BOROVKOV**, and others known and unknown to the Grand Jury, planned a series of meetings at Cafe Shokoladnitsa in the Sofia Shopping Center in Moscow.

COUNT 2
(Wire Fraud Conspiracy)

Introduction

44. Paragraphs 1 through 21 and 28 through 43 of Count One are hereby realleged and incorporated by reference herein as though fully set forth in this Count of the Superseding Indictment.

The Scheme to Defraud

45. Beginning no later than in or around December 2020 and lasting through the date of this Superseding indictment, in the District of Maryland and elsewhere, the defendants,

**AMIN STIGAL,
VLADISLAV BOROVKOV
DENIS DENISENKO,
YURIY DENISOV,
DMITRIY GOLOSHUBOV, and
NIKOLAY KORCHAGIN**

knowingly and willfully devised and intended to devise a scheme and artifice to defraud the governments of various nations, including the healthcare and transportation sectors, as well as corporate entities and to obtain money and property from those governments and entities by means of materially false and fraudulent pretenses, representations and promises (“the scheme to defraud”), in that the defendants used fraudulent credentials to access computer systems and used fraudulent identities to create accounts for the purposes of obtaining unlawful access to computer systems and obtaining the data stored on those systems from the governments and entities, and then offer that data for sale on the Internet.

The Conspiracy and the Scheme to Defraud

46. Beginning no later than in or around December 2020, and lasting through the date of this Superseding Indictment, in the District of Maryland and elsewhere, the defendants,

**AMIN STIGAL,
VLADISLAV BOROVKOV
DENIS DENISENKO,
YURIY DENISOV,
DMITRIY GOLOSHUBOV, and
NIKOLAY KORCHAGIN**

and their co-conspirators, known and unknown to the Grand Jury, did unlawfully, willfully, and knowingly combine, conspire, confederate, and agree with each other and other persons known and unknown to the Grand Jury to commit wire fraud, to wit: to knowingly execute and attempt to execute the scheme to defraud through the use of wires in interstate or foreign commerce in violation of Title 18, United States Code, Section 1343 (the “conspiracy to defraud”).

Manner and Means of the Conspiracy and Scheme to Defraud

47. It was part of the conspiracy and scheme to defraud that in or about December 2020, the Conspirators created an account for use in future cyberattacks by sending and causing to be sent fraudulent wire communications from outside the United States to servers located within the United States.

48. It was further part of the conspiracy and scheme to defraud that from in or about August 2021, through the date of this Superseding Indictment, the Conspirators scanned protected computers worldwide for possible vulnerabilities, including in the District of Maryland, as a preliminary step toward gaining unauthorized access to those protected computers.

49. It was further part of the conspiracy and scheme to defraud that beginning in or around August 2021, through October 2021, the Conspirators scanned more than 2,400 public facing Ukrainian Government websites for potential vulnerabilities, including Diia.gov.ua (DIIA),

the website for a Ukrainian Government application that was built in partnership with the United States and allowed the Ukrainian people to connect with Ukrainian Government services and access Ukrainian Government documents.

50. It was further part of the conspiracy and scheme to defraud that from on or about September 17, 2021, through on or about January 28, 2022, **STIGAL** created or caused to be created five accounts on Company 1's servers for the purpose of use in the Conspirators' attacks using fictitious identities to register the accounts. **STIGAL** did so by causing a wire to be sent from outside the United States to a server located inside the United States.

51. It was further part of the conspiracy and scheme to defraud that in or about January 2022, the Conspirators hacked into Ukrainian government systems and exfiltrated personal data associated with individuals.

52. It was further part of the conspiracy and scheme to defraud that within hours of the WhisperGate attack, on or about January 13, 2022, the Conspirators listed for sale data described as originating from the Ukrainian Government on forums across the darknet, using the moniker "Free Civilian," including:

- a. Criminal records obtained from Ukrainian Government systems;
- b. Patient health data from Ukrainian Government systems; and
- c. Motor Insurance Bureau information from Ukrainian Government systems.

53. It was further part of the conspiracy and scheme to defraud that on that same day, the Conspirators offered for sale on the Internet data for 13.5 million users from Diia.gov.ua for \$80,000.

54. It was further part of the conspiracy and scheme to defraud that the Conspirators probed protected computers in other countries for potential vulnerabilities, including from on or about August 5, 2021, through on or about February 3, 2022, the probing of public-facing websites hosted by protected computers and unassigned servers maintained by a U.S. Government Agency located in Maryland, 63 times. This probing was accomplished by sending an electronic communication from a computer located outside the United States to a computer located in Maryland.

55. It was further part of the conspiracy and scheme to defraud that in October 2022, the Conspirators probed computer networks associated with Central European Country 1's transportation sector.

56. It was further part of the conspiracy and scheme to defraud that as a result of the vulnerabilities the Conspirators discovered from their probing activities, and using fraudulent login credentials belonging to legitimate system users which the Conspirators had obtained, the Conspirators gained unauthorized access to protected computers associated with Central European Country 1's transportation sector in or around October 2022.

18 U.S.C. § 1349

FORFEITURE ALLEGATION

The Grand Jury for the District of Maryland further finds that:

1. Pursuant to the Federal Rule of Criminal Procedure 32.2, notice is hereby given to the defendant that the United States will seek forfeiture as part of any sentence in accordance with 18 U.S.C. §§ 981(a)(1)(C), 982(a)(2), and 1030(i), 28 U.S.C. § 2461(c) and 21 U.S.C. § 853(p) in the event of the defendant's conviction on the offense charged in Counts One and Two of this Superseding Indictment.

2. Upon conviction of the offenses set forth in Counts One and Two, the defendants,

**AMIN STIGAL,
VLADISLAV BOROVKOV
DENIS DENISENKO,
YURIY DENISOV,
DMITRII GOLOSHUBOV, and
NIKOLAI KORCHAGIN,**

shall forfeit to the United States, pursuant to 18 U.S.C. §§ 981(a)(1)(C), 982(a)(2), and 1030(i), and 28 U.S.C. § 2461(c), any property constituting, or derived from, proceeds obtained directly or indirectly, as a result of the violations alleged in Counts One and Two, and pursuant to 18 U.S.C. § 1030(i), any personal property that was used or intended to be used to commit or to facilitate the commission of the violation alleged in Count One.

Substitute Assets

3. If any of the property described above, as a result of any act or omission of the defendant:

- 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 which cannot be divided without difficulty

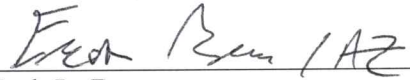
the United States shall be entitled to forfeiture of substitute property pursuant to 21 U.S.C.

§ 853(p), as incorporated by 18 U.S.C. § 982(b).

18 U.S.C. §§ 981, 982, 1030(i)

21 U.S.C. § 853(p)

28 U.S.C. § 2461(c)


Erik L. Barron
United States Attorney

SIGNATURE REDACTED

Foreperson

Date:

8-7-24