IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Holding a Criminal Term
Grand Jury Sworn in on May 25, 2021

UNITED STATES OF AMERICA	:	**CRIMINAL NO.**
	:	
v.	:	**GRAND JURY ORIGINAL**
	:	
EVGENY VIKTOROVICH GLADKIKH,	:	**VIOLATIONS:**
	:	**18 U.S.C. § 1366(a)**
Defendant.	:	**(Conspiracy To Cause Damage**
	:	**to an Energy Facility)**
	:	
	:	**18 U.S.C. § 1366(a)**
	:	**(Attempt To Cause Damage to an**
	:	**Energy Facility)**
	:	
	:	**18 U.S.C. §§ 371 and 1030(a)(2)(C),**
	:	**(a)(5)(C), (c)(2)(B)(ii), and (c)(4)(B)**
	:	**(Conspiracy To Access Protected**
	:	**Computers and Obtain Information**
	:	**and To Intentionally Damage Protected**
	:	**Computers by Knowing Transmission)**
	:	
	:	**Criminal Forfeiture:**
	:	**18 U.S.C. § 982(a)(2)(B); 18 U.S.C.**
	:	**§ 1030(i)(1)(A)-(B); 21 U.S.C. § 853(p)**

INDICTMENT

The Grand Jury charges:

At all times relevant to this Indictment:

INTRODUCTION

1. Defendant EVGENY VIKTOROVICH GLADKIKH (Евгений Викторович Гладких) ("GLADKIKH") was a resident and citizen of the Russian Federation ("Russia"), who had no residence or last known residence in the United States.

2. The STATE RESEARCH CENTER OF THE RUSSIAN FEDERATION FGUP CENTRAL SCIENTIFIC RESEARCH INSTITUTE OF CHEMISTRY AND MECHANICS ("ГОСУДАРСТВЕННЫЙ НАУЧНЫЙ ЦЕНТР РОССИЙСКОЙ ФЕДЕРАЦИИ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ ХИМИИ И МЕХАНИКИ"), known by the abbreviation "TsNIIKhM" or "CNIIHM," was a research institute of the Russian government. TsNIIKhM's website described the organization as the leading research organization of the Russian Ministry of Defense ("MoD").

3. The Applied Development Center ("ЦЕНТР ПРИКЛАДНЫХ РАЗРАБОТОК"), known by the abbreviation "ADC," was a component of TsNIIKhM engaged in, among other things, offensive and defensive cyber activity.

4. As set forth in greater detail below, GLADKIKH and co-conspirators known and unknown to the Grand Jury, including TsNIIKhM and members of TsNIIKhM and ADC, prepared, supported, conducted, and conspired to conduct computer intrusions using ADC resources that targeted energy facilities in the United States and elsewhere. Between in or around May and September 2017, they gained unauthorized access to the systems of a refinery outside the United

States using techniques and tools designed to enable an attacker to cause effects including physical damage, with potentially catastrophic effects, rather than merely causing a plant shutdown. In so doing they triggered an emergency shutdown of that facility's operations. Then, between in or around February and July 2018, GLADKIKH and co-conspirators targeted a U.S.-based company's similar facilities with similar techniques and tools and attempted to gain unauthorized access to its systems. Those 2018 attempts were unsuccessful.

A. Background Regarding Defendant, TsNIIKhM, and the Applied Development Center

5. GLADKIKH and other co-conspirators known and unknown to the Grand Jury were employed by ADC within TsNIIKhM.

6. TsNIIKhM and its predecessor organizations have a history of developing cutting-edge weapons for the Russian government and its predecessors, including the Russian Empire and the Union of Soviet Socialist Republics (U.S.S.R.). The earliest known predecessor to TsNIIKhM, the Special Chemical Laboratory for Research on Smokeless Powders of the Okhtinsk Powder Plant, was founded in St. Petersburg, Russia, as a weapons laboratory in or around 1894. In or around 1937, the U.S.S.R. renamed the lab "NII-6" designating it as a scientific research institute. Among other things, NII-6 developed anti-tank grenades to aid the Red Army during the Second World War. TsNIIKhM uses the following symbol as its logo:

7. After the Second World War, NII-6 continued producing explosives, as well as missile propellants and warheads. NII-6 was renamed TsNIIKhM in 1969. Among other things, TsNIIKhM produced explosives for Soviet interceptor satellites, which were built to attack other satellites orbiting the Earth.

8. After the U.S.S.R. dissolved, TsNIIKhM primarily engaged in civilian projects until 2005. In or around 2005, TsNIIKhM became subordinate to the MoD, Federal Service for Technical and Export Control ("Федеральной Службы По Техническому И Экспортному Контролю"), known as FSTEK.

9. Within the MoD, TsNIIKhM emphasized high-level mathematics, with specific applications in space warfare and cyber operations. In or around 2009, TsNIIKhM was assigned as the leading institute for development of new advanced weapons and was instrumental in weapons modernization. TsNIIKhM emerged as a premier MoD research and development facility working on cutting-edge space weapons and cyber capabilities.

10. TsNIIKhM was divided into divisions that are responsible for research relating to, among other subjects: satellites; nanotechnology; advanced rocket technology; protecting critical infrastructure from cyber threats; and development of weapons and special military equipment. TsNIIKhM also officially collaborates with Russian research and development institutes engaged in cyber capabilities, physics, chemistry, military, and industrial research.

11. The component of TsNIIKhM referred to as ADC publicly stated that its mission was to engage in research related to information technology-related threats to critical infrastructure. ADC publicly asserted that its research was defensive.

B. Industrial Control Systems, Operational Technology, and Safety Instrumented Systems

12. Systems that control industrial processes and ensure that they operate safely are called Industrial Control Systems ("ICS") or Operational Technology ("OT") systems.

13. Human operators remotely monitor and control ICS and OT through a Distributed Control System ("DCS"). A DCS connects an information technology ("IT") network to the OT network. A DCS consists of a computer, which can be accessible over the Internet; a controller, which is a computer that controls a physical device; and software applications. One type of DCS device is an "Engineering Workstation," which configures, maintains, and monitors applications and equipment.

14. A Safety Instrumented System ("SIS") monitors the status of DCS-controlled processes. If those processes function in an unsafe manner, the SIS attempts to bring the processes back into a safe state or performs a "safe shutdown" of the process.

15. "Triconex" is the name of SIS equipment developed and sold by Schneider Electric, a multinational corporation based in France that produces, among other things, automated systems for the energy sector. The Triconex SIS and other Schneider Electric ICS/OT products are used globally, including within the United States, across the energy and other critical/non-critical infrastructure sectors.

C. Overview of the Criminal Scheme

16. Between no later than in or about August 2014 and continuing through at least in or after July 2018, GLADKIKH, TsNIIKhM, and other co-conspirators known and unknown to the Grand Jury, who were located outside the United States, conspired to commit computer intrusions targeting energy facilities, including refineries in the United States and overseas, and to cause damage to those facilities. The conspiracy specifically targeted OT and SIS computer

systems and sought to install malicious software applications ("malware") designed to cause physical safety systems to cease operating or to operate in an unsafe manner.

a. The TRITON Computer Intrusion Scheme Targeting VICTIM COMPANY 1 Refinery

17. VICTIM COMPANY 1 was a foreign corporation engaged in, among other things, petroleum refining. VICTIM COMPANY 1 operated a refinery that utilized Triconex SIS devices for monitoring and managing the physical safety of systems including burner management systems, which facilitate safe initiation, operation, and shut-down of power generation furnaces, and sulfur recovery, which is a means of managing hazardous gas produced by crude oil refining. GLADKIKH later demonstrated a specific interest in sulfur recovery units.

18. As described below, GLADKIKH and co-conspirators gained unauthorized access to and installed a package of malware on protected computers belonging to VICTIM COMPANY 1 at a refinery facility operated by VICTIM COMPANY 1. The malware was designed to give an unauthorized operator access to and control of a Triconex device, including the ability to load additional software. That malware later became known as "TRITON" or "TRISIS" in the computer security industry.

19. On or about August 12, 2014, an individual at TsNIIKhM accessed an online service used to test whether malicious files are detectable by computer security services. The actor uploaded a malware file that was a modified version of a tool called "cryptcat," which is an open source tool used to create a back door on a compromised computer to allow continued access. Through this upload, the actor sought to determine whether computer network security tools (*e.g.*, anti-virus programs) were likely to detect the modified version of cryptcat.

20. On or about April 6, 2017, an individual at TsNIIKhM accessed the online test service and uploaded the same modified version of cryptcat that an individual at TsNIIKhM previously uploaded in 2014.

21. Beginning no later than May 2017, GLADKIKH gained unauthorized access to the IT network of VICTIM COMPANY 1's refinery. Among other things, GLADKIKH accessed technical Triconex SIS log files. GLADKIKH also sought to disable VICTIM COMPANY 1's cybersecurity systems, which were designed to prevent unauthorized access to VICTIM COMPANY 1's networks.

22. In or about May 2017, GLADKIKH and co-conspirators attempted to execute the modified version of cryptcat described above on VICTIM COMPANY 1's computer network, which showed a "file last modified" date of August 12, 2014—matching the date of the first cryptcat upload by an individual at TsNIIKhM to the online test service referenced above. The modified version of cryptcat file detected on VICTIM COMPANY 1's computer network had the same hash value—indicating an identical copy—as the modified version of cryptcat that had been uploaded to the online test service.

23. On or about May 23, 2017, GLADKIKH began seeking information regarding specific software designed to run network servers. At that time, such software was out of date, but was still used on some "historian" servers at VICTIM COMPANY 1, which were used to log historical events on the OT network and connected devices such as the SIS.

24. On or about May 24, 2017, GLADKIKH further familiarized himself with the format of log files used for Triconex devices.

25. On or about May 29, 2017, GLADKIKH used a historian server at VICTIM COMPANY 1 ("MACHINE 1") and stolen administrator login credentials to remotely access an

Engineering Workstation ("MACHINE 2") without authorization. MACHINE 2 was part of the DCS at VICTIM COMPANY 1's refinery and was connected to SIS devices, including the Tristation engineering workstation and Triconex systems.

26. Further on or about May 29, 2017, GLADKIKH installed a "back door" on MACHINE 2, which would allow an unauthorized user to gain access in the future. GLADKIKH subsequently sought information regarding protocols that would be used to communicate with a Triconex device.

27. On or about June 2, 2017, GLADKIKH and CO-CONSPIRATOR 1 familiarized themselves with a safety feature of the Triconex SIS that required a physical key to be turned to "program" mode in order for the Triconex device to allow new computer code to be installed. Normal plant running mode for the Triconex device would be in "run" mode, preventing intentional or unintentional alteration of the safety functions.

28. Further on or about June 2, 2017, GLADKIKH installed, without authorization, a package of software applications on a Triconex SIS device connected to MACHINE 2. The physical key on that device was positioned in "program" mode. Those applications comprised an early version of the TRITON malware. Within minutes of that installation, initiated by the Triconex SIS detecting a fault, an emergency shutdown of the VICTIM COMPANY 1 refinery occurred.

29. MACHINE 2 and the affected Triconex SIS provided safety controls for physical systems that handled sensitive operations including sulfur recovery and burner management systems, which could cause explosions or release toxic gases if not operated in a safe manner.

30. On or about July 17, 2017, GLADKIKH attempted to install software, without authorization, on MACHINE 1. That software was designed to gather user login credentials.

31. On or about August 4, 2017, GLADKIKH installed an updated version of the TRITON malware on a Triconex device at VICTIM COMPANY 1. The physical key on that device was positioned in "program" mode.

32. Within several hours, after the TRITON malware was copied across other Triconex SIS components, the malware caused a fault that was detected by a Triconex SIS safety feature, which in turn triggered another emergency shutdown of the VICTIM COMPANY 1 refinery.

33. On or about August 30, 2017, GLADKIKH obtained unauthorized access to a file server at VICTIM COMPANY 1 containing business records. GLADKIKH then sought information regarding a prior safety exercise at VICTIM COMPANY 1 and how VICTIM COMPANY 1 responded to that incident.

34. In summary, GLADKIKH and co-conspirators gained unauthorized access to the VICTIM COMPANY 1's DCS, and then used such access to further access the VICTIM COMPANY 1's Triconex SIS and install the package of malware known as TRITON. The TRITON malware was designed and customized to operate on the precise model of Triconex SIS devices used by VICTIM COMPANY 1. By installing the TRITON malware on VICTIM COMPANY 1's Triconex SIS, GLADKIKH and co-conspirators caused damage to the property of VICTIM COMPANY 1.

35. The methods and tools GLADKIKH and co-conspirators used demonstrate that, rather than seeking to simply cause a shutdown, they intended to gain the capability to prevent safety systems from functioning and to cause physical damage to the refinery, with potentially catastrophic effects. In particular, GLADKIKH and co-conspirators gained the capability to cause a shutdown when they gained unauthorized access to VICTIM COMPANY 1's DCS. By further expanding their unauthorized access to VICTIM COMPANY 1's SIS, GLADKIKH and co-

conspirators obtained the additional capability to cause physical damage by disabling or altering the safety shutdown functions that would normally stop a refinery from catastrophic failure.

36. In addition, GLADKIKIH and co-conspirators could have used less sophisticated malware and tools if they had intended to simply cause a shutdown. Instead, GLADKIKH and co-conspirators developed and used malware, including TRITON and other tools, that was designed to enable an attacker to load software onto the Triconex SIS devices in order to alter the safety performance of the SIS; to take physical control of the ICS at VICTIM COMPANY 1; and to cause the ICS to operate in an unsafe manner while maintaining the appearance that the ICS was operating normally. Such additional capabilities, which were custom-built into the TRITON malware that GLADKIKH and his co-conspirators used, could be employed to cause property damage, economic harm, as well as physical injury and death to individuals in close proximity to the targeted energy facility.

b. The Attempted Computer Intrusion Scheme Targeting U.S. COMPANY 1

37. On or about February 22, 2018, an individual at TsNIIKhM accessed a public website operated by the U.S. Department of Defense and viewed a technical research paper written in the 1970s for the Office of Civil Defense ("PAPER 1"). Among other things, PAPER 1 contained an extensive survey of U.S. refineries and their vulnerabilities, including an analysis of explosion and fire risk in refinery operations. PAPER 1 listed states that contained the greatest refining capacity in the United States, and where such capacities were most concentrated.

38. On or about March 2, 2018, an individual at TsNIIKhM accessed a public website operated by the U.S. Department of Defense and viewed a technical research paper written in the 1960s for the Office of Civil Defense, which contained a Department of Defense assessment of vulnerabilities of the U.S. petroleum refining industry to attack ("PAPER 2"). PAPER 2 examined

a small number of refineries in detail, discussed their vulnerabilities, and assessed the probable damage that a nuclear attack or other disaster would cause to each.

39. Several refineries that were prominently mentioned in PAPER 1 and PAPER 2 were acquired by U.S. COMPANY 1. U.S. COMPANY 1 is a U.S.-based corporation conducting business in the oil and energy sectors and operating multiple refineries in the United States. Two of the refineries owned by U.S. COMPANY 1 that were discussed in PAPERS 1 and 2 were updated to operate as sulfur recovery plants no later than the 1970s.

40. On or about March 6, 2018, GLADKIKH used a Virtual Private Network ("VPN") to conduct online reconnaissance of U.S. COMPANY 1 facilities by reviewing information that U.S. COMPANY 1 had made publicly available, including: (i) information about two of U.S. COMPANY 1's refineries that had been listed in PAPERS 1 and 2, both of which contained sulfur recovery systems; and (ii) job postings at U.S. COMPANY 1 that could potentially identify ICS equipment used at U.S. COMPANY 1 facilities. Because job postings refer to specific expertise and experience an employer seeks, reviewing job postings is a common tool used by malicious online actors to learn about equipment and processes that potential victims use. Malicious actors can use this knowledge to research and identify vulnerabilities that they can then seek to exploit. GLADKIKH also accessed web subdomains pertaining to two of U.S. COMPANY 1's U.S.-based refineries that were listed in the papers referenced above.

41. Approximately 20 minutes later, GLADKIKH initiated numerous instances of Structured Query Language ("SQL") injection attempts targeting protected computers belonging to U.S. COMPANY 1. These attempts were not successful. Shortly after the SQL injection attempts concluded, an individual at TsNIIKhM again accessed the web subdomain for one of the U.S. COMPANY 1 refineries referenced above.

42. SQL is used to store data in databases. A successful SQL injection can allow an actor to gain unauthorized access to a database, which enables the actor to read and write information, execute administrative operations, and issue commands to the operating system. SQL injection attacks can be used to obtain login credentials, steal data, erase data, or change data.

43. On or about March 16, 2018, GLADKIKH initiated another series of SQL injection attempts, targeting protected computers belonging to U.S. COMPANY 1. Those attempts were not successful.

44. On or about April 17, 2018, GLADKIKH sought information regarding U.S. COMPANY 1 and specifically regarding one of the U.S. COMPANY 1 refineries referenced above.

45. On or about July 5, 2018, GLADKIKH scanned protected computers belonging to U.S. COMPANY 1 for vulnerabilities that could enable unauthorized access to its network.

46. On or about July 30, 2018, GLADKIKH familiarized himself with the specific network security system used by U.S. COMPANY 1.

47. That same day, on or about July 30, 2018, GLADKIKH engaged in further vulnerability scanning of protected computers belonging to U.S. COMPANY 1.

COUNT ONE
(Conspiracy To Cause Damage to an Energy Facility)

48. Paragraphs 1 through 47 are re-alleged and incorporated herein.

49. From at least on or about August 12, 2014 and continuing through at least on or about July 30, 2018, beginning outside of the jurisdiction of any particular State or district and, pursuant to 18 U.S.C. §§ 3237 and 3238, within the venue of the United States District Court for the District of Columbia, the defendant, EVGENY VIKTOROVICH GLADKIKH, together with other co-conspirators known and unknown to the Grand Jury, including TsNIIKhM and members

of TsNIIKhM and ADC, did knowingly and willfully combine, conspire, confederate and agree to violate Title 18, United States Code, Section 1366(a), by damaging and attempting to damage the property of an energy facility in any amount and causing and attempting to cause a significant interruption and impairment of a function of an energy facility, that is, an energy facility belonging to U.S. COMPANY 1, in violation of Title 18, United States Code, Section 1366(a).

(Conspiracy To Cause Damage to an Energy Facility, in violation of Title 18, United States Code, Section 1366(a))

COUNT TWO
(Attempt To Cause Damage to an Energy Facility)

50. Paragraphs 1 through 47 are re-alleged and incorporated herein.

51. From at least on or about March 6, 2018, and continuing through at least on or about July 30, 2018, beginning outside of the jurisdiction of any particular State or district and, pursuant to 18 U.S.C. §§ 3237 and 3238, within the venue of the United States District Court for the District of Columbia, the defendant, EVGENY VIKTOROVICH GLADKIKH, did knowingly and willfully attempt to damage the property of an energy facility in any amount and attempt to cause a significant interruption and impairment of a function of an energy facility, that is, an energy facility belonging to U.S. COMPANY 1, in violation of Title 18, United States Code, Section 1366(a).

(Attempt To Cause Damage to an Energy Facility, in violation of Title 18, United States Code, Section 1366(a))

COUNT THREE
(Conspiracy To Access Protected Computers and Obtain Information and To Intentionally Damage Protected Computers by Knowing Transmission)

52. Paragraphs 1 through 47 are re-alleged and incorporated herein.

The Conspiracy

53. From at least on or about August 12, 2014 and continuing through at least on or about July 30, 2018, outside of the jurisdiction of any particular State or district and, pursuant to 18 U.S.C. § 3238, within the venue of the United States District Court for the District of Columbia, the defendant, EVGENY VIKTOROVICH GLADKIKH, together with other co-conspirators known and unknown to the Grand Jury, including TsNIIKhM and members of TsNIIKhM and ADC, did knowingly and willfully combine, conspire, confederate and agree to commit the following offenses against the United States:

a. In furtherance of a criminal and tortious act in violation of the Constitution and the laws of the United States, that is, causing damage to an energy facility, in violation of Title 18, United States Code, Section 1366(a), intentionally accessed, and attempted to access, computers without authorization, and thereby obtained, and attempted to obtain, information from protected computers, such conduct having involved an interstate and foreign communication, in violation of Title 18, United States Code, Section 1030(a)(2)(C) and (c)(2)(B)(ii); and

b. Knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct, intentionally caused, and attempted to cause, damage without authorization to protected computers, and caused, and attempted to cause, more than $5,000 in loss in one year, and caused, and

attempted to cause, physical injury to any person, and caused, and attempted to cause, a threat to public health or safety, in violation of Title 18, United States Code, Section 1030(a)(5)(A) and (c)(4)(B);

all in violation of Title 18, United States Code, Sections 371, 1030(a)(2)(C) and (c)(2)(B)(ii), and Sections 1030(a)(5)(A) and (c)(4)(B).

Object of the Conspiracy

54. It was the object of the conspiracy for the defendant, GLADKIKH, together with his co-conspirators, to obtain unauthorized access to protected computers belonging to energy facilities in the United States and elsewhere, including information stored on such computers, in order to cause damage and attempt to cause damage to such computers and to such energy facilities and to cause a significant interruption and impairment of a function of such energy facilities.

Manner and Means

55. Among the manner and means by which GLADKIKH and his co-conspirators would and did carry out the objectives of the conspiracy were the following:

a. They would attempt to and did obtain unauthorized access to protected computers using stolen login credentials, SQL injection attempts, and vulnerability scans.

b. Using such unauthorized access, they would attempt to and did:

    a. install software without authorization to create "back doors" on protected computers to allow persistent unauthorized access;

    b. install and delete files without authorization on protected computers; and

c. install unauthorized software on protected computers comprising Safety Instrumented Systems, which in turn enabled them to send unauthorized commands to Industrial Control Systems, and could be further used to cause property damage, economic harm, physical injury, and death.

Overt Acts

56. In furtherance of the conspiracy, and to accomplish its objects, GLADKIKH, together with other co-conspirators known and unknown to the Grand Jury, including TsNIIKhM and members of TsNIIKhM and ADC, committed and caused to be committed various overt acts beginning outside the jurisdiction of any particular State or district, including the overt acts described in paragraphs 19 through 28, 30, 31, 33, 37, 38, 40, 41, and 43 through 47, which paragraphs are re-alleged and incorporated herein.

(Conspiracy To Access Protected Computers and Obtain Information and To Intentionally Damage Protected Computers by Knowing Transmission, in violation of Title 18, United States Code, Sections 371, 1030(a)(2)(C) and (c)(2)(B)(ii), and 1030(a)(5)(A) and (c)(4)(B))

FORFEITURE ALLEGATION

1. Upon conviction of the offense charged in Count Three, the defendant shall forfeit to the United States any property, real or personal, constituting or derived from, any proceeds that the defendant obtained, directly or indirectly, as a result of such violation, pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i)(1)(B). The United States will also seek a forfeiture money judgment for a sum of money equal to the value of any proceeds that the defendant obtained, directly or indirectly, as a result of the offense charged in Count Three.

2. Upon conviction of the offense charged in Count Three, the defendant shall forfeit to the United States the defendant's interest in any personal property that was used or intended to

be used to commit or to facilitate the commission of such violation, pursuant to Title 18, United States Code, Section 1030(i)(1)(A). The United States will also seek a forfeiture money judgment for a sum of money equal to the value of any personal property that was used or intended to be used to commit or to facilitate the commission of the offense charged in Count Three.

3. If any of the property described above as being subject to forfeiture, 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 or 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;

the defendant shall forfeit to the United States any other property of the defendant, up to the value of the property described above, pursuant to Title 21, United States Code, Section 853(p).

(Criminal Forfeiture, pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i)(1)(A)-(B); and Title 21, United States Code, Section 853(p))

A TRUE BILL:

FOREPERSON.

ATTORNEY OF THE UNITED STATES IN
AND FOR THE DISTRICT OF COLUMBIA