UNITED STATES DISTRICT COURT

District of Kansas

(Kansas City Docket)

UNITED STATES OF AMERICA,

Plaintiff,

v.

CASE NO. 21-20047-HLT/JPO
~~**FILED UNDER SEAL**~~

PAVEL ALEKSANDROVICH AKULOV, MIKHAIL MIKHAILOVICH GAVRILOV, and MARAT VALERYEVICH TYUKOV

Defendants.

INDICTMENT

THE GRAND JURY CHARGES:

INTRODUCTION

1. At all times relevant to the indictment, from at least in and around July 2012 through at least in and around November 2017, the Russian Federation ("Russia") operated an intelligence and law enforcement agency called the Federal Security Service ("FSB"). The FSB was headquartered in Moscow, Russia, and was comprised of multiple units, including Military Unit 71330, which was also known within the FSB as "Center 16." The Conspirators in this case are members of a discrete operational unit within Center 16 known

by cybersecurity researchers as "Dragonfly," "Berzerk Bear," "Energetic Bear," and "Crouching Yeti." FSB Center 16 was primarily located at 12 Prospekt Vernadskogo in Moscow, Russia.

2. Defendants PAVEL ALEKSANDROVICH AKULOV (Павел Александрович Акулов), MIKHAIL MIKHAILOVICH GAVRILOV (Михаил Михайлович Гаврилов), and MARAT VALERYEVICH TYUKOV (Марат Валерьевич Тюков) were FSB officers working for Center 16. The Defendants, along with other members of FSB Center 16, knowingly and intentionally conspired with each other and with persons known and unknown to the grand jury (collectively, the "Conspirators") to undertake a sophisticated campaign to target and compromise (*i.e.*, "hack") and maintain persistent access to the networks of critical infrastructure and energy companies worldwide, including in the District of Kansas. Cybersecurity researchers referred to the two phases of the Conspirators' campaign relevant to the allegations herein as: (i) "Dragonfly" or "Havex"; and (ii) "Dragonfly 2.0."

3. A common theme of both campaign phases was the Conspirators' focus on software and hardware that controls equipment in power generation facilities, known as Industrial Control Systems ["ICS"] or Supervisory Control and Data Acquisition systems ["SCADA"] systems. During the Havex phase, the Conspirators compromised the computer networks of ICS/SCADA manufacturers and software providers and then hid their malware inside the legitimate software updates for such systems (known as a "supply chain attack"). Upon being downloaded by unsuspecting customers, the Conspirators' malicious software, among other functions, located and compromised the customers'

ICS/SCADA systems. Through such efforts, as well as other techniques, the Conspirators installed malware on more than 17,000 unique devices in the United States and elsewhere, including ICS/SCADA controllers used by power and energy companies.

4. During the later Dragonfly 2.0 phase, the Conspirators transitioned to more targeted compromises that focused on specific energy sector entities or individuals and engineers who worked in or with ICS/SCADA systems. Such efforts included: (i) spearphishing attacks, often with SCADA themes, targeting more than 3,300 users at more than 500 U.S. and international companies and entities; and (ii) compromising servers hosting websites commonly visited by engineers in the energy sector or otherwise involved in ICS/SCADA system manufacturing and then using these websites to deploy malware onto the engineers' (or other visitors') computers (known as a "watering hole attack").

5. Regardless of the evolution of the Conspirators' methods of compromise, the Conspirators' goals remained the same: to establish and maintain surreptitious, unauthorized access to networks, computers, and devices of companies and other entities in the energy sector, including power generation facilities, in the United States and elsewhere. Such accesses enabled the Russian government to disrupt and damage such systems, if it wished.

6. Images of Defendants are included below:

Pavel Aleksandrovich Akulov
(Павел Александрович Акулов)

Mikhail Mihailovich Gavrilov
(Михаил Михайлович Гаврилов)

Marat Valeryevich Tyukov
(Марат Валерьевич Тюков)

THE VICTIMS

7. The vast majority of companies targeted (and, in many cases, compromised) by the Conspirators were hundreds of U.S. and international energy sector companies and small commercial companies working with the energy sector, including companies that provide software and hardware used to control ICS/SCADA systems. The Conspirators also compromised and used, without authorization, the computers and networks of other companies, some of which had no ties to the energy industry, to serve as proxies to conduct and attempt to conduct intrusions into energy sector targets.

8. The following are examples from among hundreds of U.S.-based companies and organizations that were victims and targets of the conspiracy:

a. the Nuclear Regulatory Commission ("NRC"), a U.S. government agency responsible for regulating entities that use nuclear materials, including nuclear power plants;

b. Wolf Creek Nuclear Operating Corporation ("Wolf Creek"), a company located in Burlington, Kansas, that operates the Wolf Creek Generating Station, a nuclear power plant;

c. Westar Energy, a company located in Topeka, Kansas, which was one of the owners of Wolf Creek during the conspiracy;

d. Kansas Electric Power Cooperative ("KEPCO"), a member-owned not-for-profit power generation and transmission electric cooperative located in Topeka, Kansas, which was one of the owners of Wolf Creek during the conspiracy;

e. Company One, a data storage company located in the Midwestern United States;

f. Company Three, a commercial construction company located in Michigan;

g. Company Four, a renewable energy company located in New York;

h. Company Five, a renewable energy company located in New England;

i. Company Six, an Illinois-based media company that produces publications and websites catering to engineers in the manufacturing, oil and gas, and industrial control systems industries;

j. Company Seven, a company located in Pennsylvania that provides digital high-definition cable and high-speed internet;

k. Company Eight, an energy company located in Illinois;

l. Company Nine, an energy company located in Ohio; and,

m. Company Ten, a U.S. company that specializes in providing consulting services to nuclear power providers.

9. Additionally, hundreds of foreign victims and targets of the conspiracy were based in over 135 countries, including: Albania, Australia, Belgium, Brazil, Canada, China, Croatia, Denmark, Finland, France, Germany, Hungary, India, Ireland, Italy, the Netherlands, New Zealand, Norway, Pakistan, Singapore, Slovakia, South Africa, South Korea, Spain, Sweden, Switzerland, and the United Kingdom. This group included global oil and gas firms, utility and electrical grid companies, nuclear power plants, renewable energy companies, consulting and engineering groups, and advanced technology firms.

10. One of the victim companies based outside the United States was Company Two, a global SCADA and industrial automation company.

THE DEFENDANTS

11. Defendant PAVEL ALEKSANDROVICH AKULOV was a Russian military officer assigned to Military Unit 71330 and held the rank of lieutenant as of 2013. AKULOV conducted online reconnaissance in support of the Conspirators' spearphishing campaigns, including reconnaissance supporting the Conspirators' targeting of, and unauthorized access to, Wolf Creek's computer network (part of Dragonfly 2.0).

12. Defendant MIKHAIL MIKHAILOVICH GAVRILOV was a Russian military intelligence officer assigned to Military Unit 71330. During his tenure with the unit, GAVRILOV held the position of captain and, later, major. GAVRILOV conducted,

at least in part, computer intrusions into Wolf Creek's computer network, as well as computer intrusions against Company Seven's computer network, which the Conspirators used to access various energy, utility, and critical infrastructure webmail login webpages (both part of Dragonfly 2.0).

13. Defendant MARAT VALERYEVICH TYUKOV was a Russian military intelligence officer assigned to Military Unit 71330. TYUKOV engaged in unauthorized access to a server owned by Company One, which he, at least in part, used to manage command and control ("C2") infrastructure. TYUKOV also engaged in computer intrusions against Company Two's computer network. The Conspirators then laced updates for Company Two's industrial control software with malware, where it was available for download by power and energy companies worldwide, including in the United States (part of Dragonfly/Havex).

COUNT 1

CONSPIRACY TO CAUSE DAMAGE TO THE PROPERTY OF AN ENERGY FACILITY; TO GAIN UNLAWFUL ACCESS AND OBTAIN INFORMATION FROM A PROTECTED COMPUTER; TO DAMAGE A PROTECTED COMPUTER; AND TO ACCESS A NON-PUBLIC COMPUTER OF A GOVERNMENT AGENCY WITHOUT AUTHORIZATION
[18 U.S.C. § 371]

14. The allegations contained in paragraphs 1 through 10 are repeated, re-alleged, and incorporated by reference as if fully set forth herein.

15. Beginning at least in and around July 2012 and continuing through at least in and around November 2017, the exact dates being unknown to the grand jury, in the District of Kansas and elsewhere, the defendants,

knowingly and intentionally combined, conspired, confederated, and agreed together, with each other and with others known and unknown to the grand jury, to commit the following offenses against the United States:

a. to knowingly and willfully cause damage to the property of an energy facility that would have, if completed, caused a significant interruption and impairment in the function of such energy facility, in violation of Title 18, United States Code, Section 1366;

b. to access a computer without authorization and to obtain thereby information from a protected computer, in furtherance of a criminal and tortious act in violation of the laws of the United States, that is, conspiracy to commit wire fraud, in violation of Title 18, United States Code, Section 1349, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B)(ii);

c. to knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, to cause damage without authorization to a protected computer, and where the offense did cause and would, if completed, have caused loss aggregating more than $5,000 in value to at least one person during a one-year period from a related course of conduct affecting a protected computer and damage affecting at least 10 protected computers during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B); and

d. to intentionally, without authorization, access a non-public computer of a department or agency of the United States, namely, the NRC, that is exclusively for the use of the Government of the United States, in violation of Title 18, United States Code, Sections 1030(a)(3) and 1030(c)(2)(A).

16. All in violation of Title 18, United States Code, Sections 371 and 2.

OBJECT OF THE CONSPIRACY

17. The object of the conspiracy was to establish and maintain surreptitious, unauthorized access to networks, computers, and devices of companies and other entities in the energy sector, including power generation facilities, in the United States and elsewhere, thereby enabling the Russian government to disrupt and damage such systems, if it wished.

MANNER AND MEANS OF THE CONSPIRACY

18. To avoid detection by law enforcement, security researchers, and victims, and to mask their FSB affiliation and location in Russia, the Conspirators used a variety of fictitious names and personas, as well as online infrastructure (including servers, domains, email accounts, and other online services), provided by and belonging to companies in the United States and elsewhere.

19. The Conspirators used this infrastructure, frequently without authorization, for a wide range of conduct in furtherance of the conspiracy, including the methods identified below, internal communications, reconnaissance and research about energy sector victims, and the storage, management, and distribution of hacking tools and malware.

20. The Conspirators often initiated their hacking activities by researching victim organizations and probing their computer networks. This reconnaissance provided technical and biographical information that the Conspirators could exploit in targeting their computer intrusion victims.

21. In some cases, the Conspirators gained unauthorized access to victim devices and networks through a particular malware package (known publicly as "Havex") that was designed to compromise computers, networks, and ICS/SCADA devices. Among other things, Havex allowed the Conspirators to install backdoor access to compromised devices and networks. One of the ways the Conspirators spread Havex to more than 17,000 unique devices worldwide was by inserting Havex into otherwise legitimate ICS/SCADA software through supply chain attacks.

22. The Conspirators also gained unauthorized access to targeted victim networks by exploiting a vulnerability in a particular security software package (the "Security Software Vulnerability") that allowed for remote code execution – *i.e.*, the Conspirators could run unauthorized programs on the victim machine. While the specific vulnerability used by the Conspirators is unknown, it is likely that at some victims had not installed available software patches. The Conspirators then used such access to create administrator accounts on victim networks. Examples of U.S.-based victims that were compromised through this method include Company Three and Company Seven.

23. In some cases, the Conspirators used administrator-level privileges (*e.g.*, privileges obtained using the Security Software Vulnerability) to access victim networks through remote desktop protocol ("RDP") connections and to create company email

accounts. They then used those accounts to send spearphishing emails to numerous targets, including individuals and engineers who worked in or with critical infrastructure ICS/SCADA systems. For example, the Conspirators used their unauthorized access to Company Three's computer network to create email accounts for fictitious employees (*e.g.*, jon.patrick@[Company Three's corporate domain].com) and to send spearphishing e-mails to accounts at Wolf Creek, Westar Energy, NRC, Company Four, Company Eight, and Company Nine. In many cases, the Conspirators crafted these spearphishing emails to appear as though the sender was a job seeker with experience in critical infrastructure tools and protocols.

24. The Conspirators would attach a purported résumé, titled either "Controls Engineer.docx," "CV Controls Engineer.docx," or "CV [false Company Three employee name]" (the "Controls Engineer Résumés") that contained malware that would collect victims' computer credentials by leveraging a Server Message Block ("SMB") redirect vulnerability. Specifically, when a recipient opened the malicious attachment, their computer would attempt to download a file from a server controlled by the Conspirators. If the victim network's firewall did not block outbound SMB protocol traffic, the recipient's computer in many cases would attempt to authenticate to the Conspirators' server by sending the recipient's username and password hash (*i.e.*, a string of numbers that can be translated into an actual password if the recipient device has the proper algorithm or via a brute force attack). If Conspirators successfully decrypted the password via brute force, they could then use the username and password to gain unauthorized access to the network.

25. In addition, the Conspirators used spearphishing emails and publicly known vulnerabilities in popular content management software to compromise web servers hosting websites commonly visited by engineers in energy industries, including websites managed by Company Four, Company Five, and Company Six. The Conspirators used this unauthorized access to add malicious JavaScript code to the websites. These watering hole attacks allowed the Conspirators to steal the credentials of individuals who browsed the compromised websites.

26. After gaining unauthorized access to victim computers, the Conspirators installed tools and performed a variety of functions designed to maintain control and access to these computers and networks. One such tool was "Backdoor.Goodor," which is a downloader that opened a backdoor on the victim computer and beaconed to hardcoded domains controlled by the Conspirators. The Conspirators would then work to identify, collect, package, and view user credentials, all to allow the Conspirators to move laterally (*i.e.*, to additional computers within a victim network or entity) and hierarchically (*i.e.*, at increasingly higher levels of access) throughout victims' computer networks. Through such methods, the Conspirators would identify and obtain access to sensitive, private data and maintain persistent access that would enable future cyber operations, including operations designed to interfere with and damage power and power delivery systems.

COMPUTER INTRUSIONS AND OTHER OVERT ACTS

PHASE ONE: Deployment and Management of Havex Infrastructure

27. Between at least 2012 through 2014, the Conspirators used spearphishing, watering hole attacks, and supply chain attacks to deploy Havex, which they subsequently

used, in part, to map and compromise networked ICS/SCADA devices. Specifically, after infecting a computer on a network, one Havex component would automatically use the Open Communications Platform, a protocol used for Windows communications with SCADA devices, to locate ICS/SCADA devices on a targeted network.

28. Havex also allowed the Conspirators to, among other things, copy login credentials, gather user information from infected computers and devices, and install backdoors, allowing them to access and control compromised devices at will.

Compromise and Use of Company One Server as a Proxy

29. Beginning in at least July 2012, the Conspirators accessed, without authorization, a server owned by Company One ("the Company One Proxy"). From in and around July 2012 through in and around April 2013, the Conspirators maintained exclusive control of this server and used it as a proxy through which they could route their operational traffic while hiding their true location and identities as they engaged in criminal activity. While being used by the Conspirators, the server housing the Company One proxy was located in the United States.

30. The Conspirators used the Company One proxy to, among other things, create and manage a wide-ranging network of Havex C2 servers. For example, on August 28, 2012, the Conspirators used the Company One proxy to upload Havex malware control panels to three C2 servers. The Conspirators maintained exclusive access to the control panels installed on these three servers via a unique password. The Conspirators used this same password to access more than 250 other domains that they used to host Havex C2 infrastructure.

31. On or about August 30, 2012, TYUKOV used the Company One proxy to access the Havex control panels on three Havex C2 servers. After viewing the files on those servers, TYUKOV uploaded one copy of the Havex malware to each of the C2 domains.

32. While logged into the Havex control panels, TYUKOV also uploaded files for use in watering hole attacks that installed Havex and other exploits on a visitor's computer.

Target Research and SQL Injection

33. The Conspirators commonly conducted online research to identify potential targets. For example, on multiple occasions in July 2012, the Conspirators used the Company One proxy to conduct target research on the website of the International Atomic Energy Agency. One of the pages viewed by the Conspirators listed companies and agencies involved in nuclear power activities in the United States, and discussed numerous entities targeted by the Conspirators throughout the conspiracy, including the NRC, Wolf Creek, Company Eight, and Company Nine.

34. Throughout December 2012, the Conspirators repeatedly targeted the website of Company Ten via Structured Query Language (SQL) injections, an exploitation method that relies on misconfigured web applications to provide an actor with the ability to read and write information, execute administrative operations, and issue commands to the operating system.

35. Through these efforts, the Conspirators compromised Company Ten's website and obtained non-public information, including the usernames and passwords of

more than 10,000 users on Company Ten's website. Among these were hundreds of individual users at entities targeted throughout the conspiracy, including the NRC, Wolf Creek, Westar Energy, Company Eight, and Company Nine.

SCADA Manufacturer Compromise

36. In and around August 2012, TYUKOV and other Conspirators used the Company One proxy to conduct SQL injections against a website belonging to Company Two. Ultimately, TYUKOV obtained unauthorized access to nonpublic data, including internal configuration information about the server hosting Company Two's website, information about the database supporting that website, and the username and password for the website's administrator account.

37. On or about November 12, 2012, the Conspirators again accessed Company Two's server and downloaded BIOS and driver software for Company Two products.

Havex Supply Chain Attack

38. Between at least 2013 and 2014, the Conspirators caused the distribution of Havex malware inside legitimate Company Two driver software that was available for public download. Once installed, this software attempted to contact Havex C2 infrastructure. For example, a version of the compromised update software was found on a SCADA device used by a power generation plant in the United States.

PHASE TWO: Targeted Persistent Access to Victim Companies' Systems

39. In a second phase of the conspiracy, the Conspirators undertook other efforts to obtain long-term, persistent access to the computer systems of energy companies and their power generation facilities (generally referred to "Dragonfly 2.0," as noted above).

Energy Sector Spearphishing Attacks via Compromised Servers

40. In and around early 2014, the Conspirators used the Security Software Vulnerability to compromise a Michigan-based server that belonged to Company Three.

41. From in and around March 2014 through in and around October 2015, the Conspirators used this unauthorized access to create four administrator accounts on Company Three's network with usernames resembling legitimate systems or processes, such as MS_AutoUP, SYSTEM_USER, LOCAL_SYS, and SYSTEM_NT (the Conspirators also created accounts with identical names on other victim networks).

42. In and around February and March 2017, the Conspirators used one of their unauthorized administrator accounts to create four Company Three email accounts associated with fictitious names. From on or about February 28, 2017, to on or about May 31, 2017, the Conspirators used these email accounts to send spearphishing emails with malware-laced attachments to more than 3,300 email accounts associated with more than 500 U.S. and international companies and entities, primarily in the energy sector. The targets of the Conspirators' spearphishing emails included more than 170 companies and entities in the United States, in addition to hundreds of companies in and entities in Africa, Asia, Australia, Europe, the Middle East, and South America, as well as more. Some examples of the Conspirators spearphishing against U.S.-based targets include:

a. one e-mail sent on or about May 24, 2017 to an NRC account;

b. ten nearly identical emails sent on or about May 5 and 15, 2017, to eight Wolf Creek accounts belonging to eight Wolf Creek employees ("Employees 1 through 8");

c. twenty-nine emails sent on or about May 19, 2017, to nineteen KEPCO accounts;

d. nineteen emails sent on or about May 19 and 24, 2017, to nineteen Westar Energy accounts;

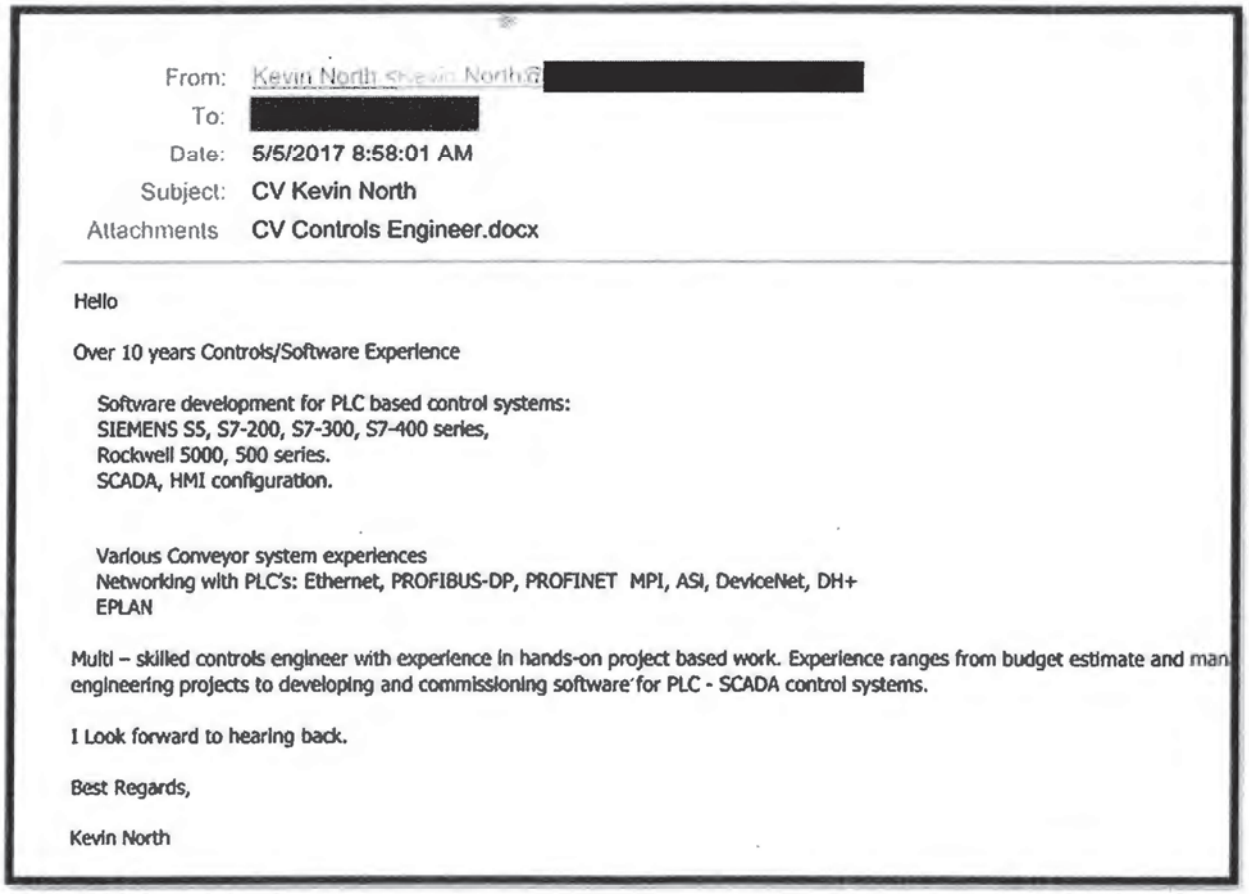
e. thirty-seven emails sent on or about May 24 and 29, 2017 to twenty-nine Company Four accounts;

f. eighteen emails sent from on or about May 11, 2017, to May 24, 2017, to fourteen Company Eight accounts;

g. three emails sent from on or about May 15, 2017, to May 24, 2017, to two accounts at Company Nine.

43. The Conspirators sent the May 5, 2017 spearphishing emails to Wolf Creek Employees 1 through 7 over the course of about five minutes, after AKULOV had conducted reconnaissance against Wolf Creek, Westar Energy, and international energy sector networks.

44. The Conspirators specifically targeted users likely to have access to ICS/SCADA data and systems, since these emails, as well as the malware-laced attachments, typically referenced SCADA systems. An example of one of these emails is included below.



From: Kevin North <kevin.North@[redacted]
To: [redacted]
Date: 5/5/2017 8:58:01 AM
Subject: CV Kevin North
Attachments CV Controls Engineer.docx

Hello

Over 10 years Controls/Software Experience

Software development for PLC based control systems:
SIEMENS S5, S7-200, S7-300, S7-400 series,
Rockwell 5000, 500 series.
SCADA, HMI configuration.

Various Conveyor system experiences
Networking with PLC's: Ethernet, PROFIBUS-DP, PROFINET MPI, ASI, DeviceNet, DH+
EPLAN

Multi – skilled controls engineer with experience in hands-on project based work. Experience ranges from budget estimate and man engineering projects to developing and commissioning software for PLC - SCADA control systems.

I Look forward to hearing back.

Best Regards,

Kevin North

45. On or about May 15, 2017, GAVRILOV assisted in drafting the spearphishing e-mail sent that day to Wolf Creek Employee 1.

46. Although many targeted users at U.S.-based entities opened the malicious attachments, most of the malicious activity was blocked by victims' network firewalls (which blocked outbound SMB protocol connections) or mitigated before the actors could leverage the stolen credentials. But, as discussed below, even a single user clicking on the malicious attachment was enough for the Conspirators to compromise a targeted company's network.

Compromise of Wolf Creek's Computer Network

47. In and around May 2017, after using the Conspirator-created Company Three accounts to send spearphishing emails to Wolf Creek email accounts as described in paragraphs 42-46, the Conspirators compromised at least one Wolf Creek user account and used that account to download and store malware on Wolf Creek's business network, which was not directly connected to any ICS/SCADA devices. The Conspirators then used this malware to move laterally across Wolf Creek's computer network and harvest additional Wolf Creek employee credentials. The servers that housed the accounts for Employees 1-8 – as well as Employee 9, discussed below – during this time were located in the District of Kansas. Further, during this time, all of Wolf Creek's internet traffic was routed through servers located in the District of Kansas.

48. Specifically, the Conspirators first obtained unauthorized access to Wolf Creek's computer network on or about May 11, 2017, by compromising Employee 1's account via the spearphishing activity described above. The Conspirators then used Employee 1's credentials to access his/her account without authorization on dozens of occasions from on or about May 11, 2017, through on or about May 17, 2017 to, among other things, maintain persistence and compromise additional accounts.

49. During this time, the Conspirators added several malicious executable files and computer scripts to Employee 1's file storage. For example, on or about May 11, 2017, minutes after first accessing Employee 1's account, the Conspirators added a malware file called ntdll.exe, which contained Backdoor.Goodor, to Employee 1's file storage. When

executed, ntdll.exe allowed the Conspirators to execute commands on victim systems via one of nine C2 servers, some of which the Conspirators also used to target other victims.

50. Later that same day, GAVRILOV placed a shortcut file (named SETROUTE.lnk) in several Wolf Creek users' file storage, including Employee 1. The Conspirators designed the shortcut files to request access to a file icon (*e.g.*, pic.png) from a Conspirator-controlled server outside Wolf Creek's network, thereby sending user credentials to those servers via an SMB redirect attack. The SMB redirect attack did not require that a user click on the malicious file. Instead, this attack would be triggered if a user opened a directory containing the shortcut file.

51. The next day, on or about May 12, 2017, after the Conspirators had obtained access to Wolf Creek's computer network, AKULOV continued to familiarize himself with Wolf Creek and Westar Energy.

52. On or about May 15, 2017, GAVRILOV added three files – svcsrv.bat, Inveigh.ps1, and Inveigh-Relay.ps1 – to Employee 1's file storage. These files were designed to exploit SMB traffic, allowing the Conspirators to collect usernames and password hashes for computers on a victim network.

53. That same day, the Conspirators added more malware – notepad.exe.lnk, d.js, and SD.bat – to the file storage of several Wolf Creek employees, including Employee 1. The Conspirators designed these files to capture additional information about a victim network and gather usernames and password hashes to aid the Conspirators' efforts to compromise Wolf Creek's network.

54. Through such methods, the Conspirators obtained access to at least one other Wolf Creek employee account, ("Employee 9"), which the Conspirators used, without authorization, from on or about May 18, 2017, through on or about May 29, 2017. As with Employee 1's account, the Conspirators used Employee 9's account to store and download malware on Wolf Creek's network.

Compromise and Creation of Energy Sector Watering Hole Domains

55. From in and around December 2016 through in and around June 2017, the Conspirators seeded at least six domains with malicious JavaScript code (since remediated) that, using an SMB redirect attack, caused computers visiting those websites to become watering holes. One of the compromised websites belonged to Company Four, another belonged to Company Five, and four belonged to Company Six. During the Conspiracy, the servers hosting these websites were located in the United States.

56. All of these websites would have been of interest to those involved in the energy sector, including power system operators. Moreover, each of these compromised websites involved information or publications of particular interest to those involved in the energy sector or the manufacture and use of ICS/SCADA devices.

57. In some cases, the Conspirators gained the necessary access to embed the malicious JavaScript code via spearphishing. For example, on May 29, 2017, the Conspirators sent a spearphishing email with a "Controls Engineer Résumés" malicious attachment to a Company Four employee who had administrative access to Company Four's website ("Employee 10"). Employee 10 opened the attachment, which caused the transmission of Employee 10's username and hashed password to the Conspirators. On or

about June 5, 2017, the Conspirators used Employee 10's credentials to access the administrative portion of Company Four's website to insert the malicious JavaScript code.

58. Alternatively, the Conspirators also gained the necessary unauthorized access through vulnerabilities in popular content management software. For example, on or about April 7, 2017, the Conspirators compromised Company Five's website in this manner.

59. These watering holes resulted in connections between several domestic energy sector companies' computer networks and the Conspirators' credential harvesting servers. This included computers at Westar Energy, which connected to one of the Conspirators' servers on April 4, 2017.

Use of Compromised Company Seven Account as a Proxy

60. On or about March 2, 2017, after the Conspirators accessed, without authorization, a Company Seven server via the Security Software Vulnerability, the Conspirators created an administrator account called MS_BACKUP on Company Seven's computer network. The Conspirators remotely accessed this account from on or about March 2, 2017, to on or about November 14, 2017. During this time, the servers hosting Company Seven's network were located in the United States.

61. The Conspirators repeatedly used Company Seven's network (via the MS_BACKUP account) as a proxy to further the conspiracy. For example, from on or about May 28, 2017, to on or about November 12, 2017, the Conspirators attempted to, and in many cases did, log into the web services of various Chinese and European energy, utility, and critical infrastructure entities.

62. Additionally, on or about September 29, 2017, GAVRILOV used the MS_BACKUP account to access some of the conspiracy's other hacking infrastructure.

COUNT 2

COMPUTER FRAUD – UNLAWFUL ACCESS TO OBTAIN INFORMATION FROM PROTECTED COMPUTERS
[18 U.S.C. §§ 1030(a)(2)(C), 1030(c)(2)(B)(ii), and 2]

63. The allegations contained in paragraphs 1 through 62 are repeated, re-alleged, and incorporated by reference as if fully set forth herein.

64. From on or about May 11, 2017, to on or about May 29, 2017, in the District of Kansas and elsewhere, the defendants,

PAVEL ALEKSANDROVICH AKULOV and
MIKHAIL MIKHAILOVICH GAVRILOV,

intentionally accessed a computer without authorization and thereby obtained information from a protected computer, in furtherance of a criminal and tortious act in violation of the laws of the United States, that is, wire fraud, in violation of Title 18, United States Code, Section 1343, and aided and abetted the same, to wit, AKULOV and GAVRILOV accessed, and aided and abetted accessing, without authorization Wolf Creek's computer network and obtained user credentials.

65. All in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B)(ii) and 2.

COUNTS 3-6

COMPUTER FRAUD – DAMAGE TO PROTECTED COMPUTERS
[18 U.S.C. §§ 1030(a)(5)(A), 1030(b), 1030(c)(4)(B), and 2]

66. The allegations contained in paragraphs 1 through 62 are repeated, re-alleged, and incorporated by reference as if fully set forth herein.

67. On or about the dates listed below, in the District of Kansas and elsewhere, the defendants,

PAVEL ALEKSANDROVICH AKULOV and
MIKHAIL MIKHAILOVICH GAVRILOV,

knowingly caused and attempted to cause the transmission of a program, information, code, and command, and as a result of such conduct, caused and attempted to cause damage without authorization to a protected computer; to wit, the defendants knowingly caused and attempted to cause the transmission of malware to computers on Wolf Creek's computer network, and aided and abetted the same, and as a result of such conduct, caused and attempted to cause damage without authorization to computers used by Wolf Creek. The offenses caused loss resulting from a related course of conduct affecting one or more protected computers aggregating at least $5,000 in value.

Count	Approximate Date	Basis
3	May 11, 2017	Transmitting the ntdll.exe file to Employee 1's user directory
4	May 11, 2017	Transmitting the SETROUTE.lnk file to multiple user directories
5	May 15, 2017	Transmitting svcsrv.bat, Inveigh.ps1, and Inveigh-Relay.ps1 to Employee 1's user directory
6	May 15, 2017	Transmitting the notepad.exe.lnk, d.js, and SD.bat files to Employee 1's and other accounts' file storage

68. Each in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(B), and 2.

COUNT 7

WIRE FRAUD CONSPIRACY
[18 U.S.C. § 1349]

69. The allegations contained in paragraphs 1 through 13 and paragraphs 18 through 62 are repeated, re-alleged, and incorporated by reference as if fully set forth herein.

THE CONSPIRACY AND ITS OBJECTS

70. Beginning at least in and around July 2012 and continuing through at least in and around November 2017, the exact dates being unknown to the grand jury, in the District of Kansas and elsewhere, the defendants,

PAVEL ALEKSANDROVICH AKULOV
MIKHAIL MIKHAILOVICH GAVRILOV, and
MARAT VALERYEVICH TYUKOV

knowingly and intentionally conspired, combined, and agreed together, with each other, and with others known and unknown to the grand jury, to commit an offense against the United States, that is, wire fraud, contrary to the provisions of Title 18, United States Code, Section 1343; to wit, the defendants, PAVEL ALEKSANDROVICH AKULOV, MIKHAIL MIKHAILOVICH GAVRILOV, and MARAT VALERYEVICH TYUKOV, together with conspirators, devised and intending to devise a scheme to defraud, and to obtain property by means of false and fraudulent pretenses, representations and promises, transmitted and caused to be transmitted by means of wire communication in interstate and

foreign commerce, certain writings, signs, signals, and pictures for the purpose of executing such scheme.

71. Specifically, an object of the conspiracy was to, by means of false and fraudulent pretenses, obtain authentication credentials to maintain persistent access to victim computer networks by hacking computers belonging to companies and entities that were part of the global energy sector, including their power generation facilities. These victims include those described in paragraphs 7 through 10 above.

72. With respect to computer intrusions that were part of the conspiracy, the Conspirators transmitted, in interstate and foreign commerce, computer code and files designed to gain unauthorized access to victims' computers and networks. After compromising victims' systems, the Conspirators sent commands to, and received communications from, computer files and malware that they had installed on victim machines.

73. For example, some of the Conspirators' intrusion activities involved supply chain attacks that spread malware via vendors that provided equipment and software to energy and power generation companies. After gaining unauthorized access to the computers of equipment vendors, the Conspirators would illegally obtain and modify victim vendors' software, and then replace the legitimate software on vendors' websites with versions that would, when installed by users, grant the Conspirators unauthorized access to victims' computers via backdoors and other malware.

74. The Conspirators also used stolen authentication credentials to misrepresent their identities within the victims' networks to obtain unauthorized access to and move

laterally within victim networks. The Conspirators also created administrator-level accounts to misrepresent their identities within the victims' networks and email accounts that mimicked those of legitimate victim accounts.

75. In addition, the Conspirators crafted and transmitted, in interstate and foreign commerce, spearphishing emails designed to gain unauthorized access to victims' computer networks. The Conspirators created spearphishing emails that appeared legitimate to deceive recipient victims into opening the emails and their malicious attachments, thus enabling the Conspirators to steal credentials for the victims' computer networks.

76. In some instances, Conspirators also compromised and then used watering hole domains, which the Conspirators used to induce victim computers to reveal credentials for the victims' computer networks and download malicious software that would gain unauthorized access to the victims' computers.

77. All in violation of Title 18, United States Code, Section 1349.

COUNTS 8 - 17

WIRE FRAUD
[18 U.S.C. §§ 1343 and 2]

78. The allegations contained in paragraphs 1 through 13 and paragraphs 18 through 62, and paragraphs 70 through 77 are repeated, re-alleged, and incorporated by reference as if fully set forth herein.

79. On or about the dates set forth below, in the District of Kansas and elsewhere, the defendants,

PAVEL ALEKSANDROVICH AKULOV and
MIKHAIL MIKHAILOVICH GAVRILOV,

having devised and intending to devise a scheme to defraud, and to obtain property by means of false and fraudulent pretenses, representations and promises, transmitted and caused to be transmitted by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, and pictures for the purpose of executing such scheme and artifice, and aided and abetted the same; to wit, the defendants knowingly transmitted malware by means of wires to Wolf Creek's computer systems, on or about the dates and times set forth below in Counts 8 through Count 17, and stole and used Employee 1's user authentication credentials to make a transmission in furtherance of adding malware to Wolf Creek's computer network, on or about the date and time set forth below in Count 17.

Count	Approximate Date (EDT)	Basis
8	May 5, 2017	Spearphishing Email Sent to Employee 2
9	May 5, 2017	Spearphishing Email Sent to Employee 3
10	May 5, 2017	Spearphishing Email Sent to Employee 1
11	May 5, 2017	Spearphishing Email Sent to Employee 4
12	May 5, 2017	Spearphishing Email Sent to Employee 5
13	May 5, 2017	Spearphishing Email Sent to Employee 6
14	May 5, 2017	Spearphishing Email Sent to Employee 7
15	May 15, 2017	Spearphishing Email Sent to Employee 1
16	May 15, 2017	Spearphishing Email Sent to Employee 8
17	May 11, 2017	First outbound transmission from Employee 1's account to an IP address controlled by the Conspirators

80. Each was in violation of Title 18, United States Code, Sections 1343 and 2.

COUNTS 18 - 20

AGGRAVATED IDENTITY THEFT
[18 U.S.C. §§ 1028A and 2]

81. The allegations contained in paragraphs 1 through 13, paragraphs 18 through 62, and paragraphs 70 through 77 are repeated, re-alleged, and incorporated by reference as if fully set forth herein.

82. On or about the dates set forth below, in the District of Kansas and elsewhere, the defendants,

PAVEL ALEKSANDROVICH AKULOV and
MIKHAIL MIKHAILOVICH GAVRILOV,

knowingly transferred, possessed and used without lawful authority, a means of identification of another person, and aided and abetted the same, during and in relation to a felony violation enumerated in Title 18, United States Code, Section 1028A(c), namely, conspiracy to commit wire fraud, in violation of Title 18, United States Code, Section 1349, as charged in Count 7, knowing that the means of identification belonged to another real person who worked on behalf of the targeted victim organization.

Count	Approximate Dates	Victim Organization	Means of Identification
18	May 11, 2017, to May 17, 2017	Wolf Creek	Username and password for account used by Employee 1
19	May 18, 2017, to May 29, 2017	Wolf Creek	Username and password for account used by Employee 9
20	May 31, 2017, to June 5, 2017	Company Four	Username and password for account used by Employee 10

83. Each in violation of Title 18, United States Code, Sections 1028A(a)(1), 1028A(b), 1028A(c)(4), and 2.

FORFEITURE NOTICE

84. The allegations contained in paragraphs 1 through 83 of this Indictment are realleged and incorporated by reference as though fully set forth herein for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Sections 981(a)(1)(C), 982(a)(2)(B), and 1030(i) and Title 28, United States Code, Section 2461.

85. Upon conviction of one or more of the offenses set forth in Counts One through Seventeen of this Indictment, the defendants shall forfeit to the United States of America, pursuant to Title 18, United States Code, Sections 981(a)(1)(C), 982(a)(2)(B), and 1030(i)(1)(B) and Title 28, United States Code, Section 2461(c), any property, real or personal, which constitutes or is derived from proceeds traceable to the offenses.

86. Upon conviction of one or more of the offenses set forth in Counts One through Six of this Indictment, the defendants shall forfeit to the United States of America, pursuant to Title 18, United States Code, Section 1030(i)(1)(A), any personal property that was used or intended to be used to commit or to facilitate the commission of such violations.

SUBSTITUTE ASSETS

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

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 which cannot be divided without difficulty,

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p).

A TRUE BILL.

August 26, 2021
DATE

s/Foreperson
FOREPERSON OF THE GRAND JURY

DUSTON J. SLINKARD
ACTING UNITED STATES ATTORNEY

MARK J. LESKO
ACTING ASSISTANT ATTORNEY GENERAL

By: /s/ Ali Ahmad,
Ali Ahmad
Counsel for Cyber Investigations
National Security Division
Main Justice Building
950 Pennsylvania Avenue, NW
Washington, D.C. 20530
Ph: (202) 514-2000
Fax: (202) 532-4251
Email: Ali.Ahmad2@usdoj.gov
NY S. Ct. No. 4428587

By: /s/ Christine Bonomo,
Christine Bonomo
Trial Attorney
National Security Division
Main Justice Building
950 Pennsylvania Avenue, NW

Washington, D.C. 20530
Ph: (202) 514-2000
Fax: (202) 532-4251
Email: Christine.Bonomo@usdoj.gov
NY S. Ct. No. B10113801

By: /s/ Scott C. Rask,
Scott C. Rask
Assistant United States Attorney
District of Kansas
500 State Avenue, Suite 360
Kansas City, Kansas 66101
Ph: (913) 551-6730
Fax: (913) 551-6541
Email: Scott.Rask@usdoj.gov
Ks. S. Ct. No. 15643

By: /s/ D. Christopher Oakley,
D. Christopher Oakley
Assistant United States Attorney
District of Kansas
500 State Avenue, Suite 360
Kansas City, Kansas 66101
Ph: (913) 551-6730
Fax: (913) 551-6541
Email: Chris.Oakley@usdoj.gov
Ks. S. Ct. No. 19248

By: /s/ Ryan J. Huschka,
Ryan J. Huschka
Assistant United States Attorney
District of Kansas
500 State Avenue, Suite 360
Kansas City, Kansas 66101
Ph: (913) 551-6730
Fax: (913) 551-6541
Email: Ryan.Huschka@usdoj.gov
Ks. S. Ct. No. 23840

IT IS REQUESTED THAT THE TRIAL BE HELD IN KANSAS CITY, KANSAS

PENALTIES

Count 1 [18 U.S.C. § 371 conspiracy]

- Punishable by a term of imprisonment of not more than five years. 18 U.S.C. § 371.
- A term of supervised release of not more than three years. 18 U.S.C. § 3583(b)(2).
- A fine not to exceed $250,000. 18 U.S.C. § 3571(b)(3).
- A mandatory special assessment of $100. 18 U.S.C. § 3013(a)(2)(A).
- Forfeiture.

Count 2 [18 U.S.C. §§ 1030(a)(2)(C) & 1030(c)(2)(B)(ii) computer fraud to obtain information]

- Punishable by a term of imprisonment of not more than five years. 18 U.S.C. § 1030(c)(2)(B).
- A term of supervised release of not more than three years. 18 U.S.C. § 3583(b)(2).
- A fine not to exceed $250,000. 18 U.S.C. § 3571(b)(3).
- A mandatory special assessment of $100. 18 U.S.C. § 3013(a)(2)(A).
- Forfeiture.

Counts 3-6 [18 U.S.C. §§ 1030(a)(5)(A) & 1030(c)(4)(B) computer fraud to damage protected computers]

- Punishable by a term of imprisonment of not more than ten years. 18 U.S.C. § 1030(c)(4)(B).
- A term of supervised release of not more than three years. 18 U.S.C. § 3583(b)(2).

- A fine not to exceed $250,000. 18 U.S.C. § 3571(b)(3). In the alternative, the defendant may be fined not more than the greater of twice the gross gain or twice the gross loss. 18 U.S.C. § 3571(d).

- A mandatory special assessment of $100. 18 U.S.C. § 3013(a)(2)(A).

- Forfeiture.

Counts 7-17 [18 U.S.C. §§ 1349 and 1343 wire fraud conspiracy and wire fraud]

- Punishable by a term of imprisonment of not more than twenty years. 18 U.S.C. § 1343.

- A term of supervised release of not more than three years. 18 U.S.C. § 3583(b)(2).

- A fine not to exceed $250,000. 18 U.S.C. § 3571(b)(3). In the alternative, the defendant may be fined not more than the greater of twice the gross gain or twice the gross loss. 18 U.S.C. § 3571(d).

- A mandatory special assessment of $100. 18 U.S.C. § 3013(a)(2)(A).

- Forfeiture.

Counts 18-21 [18 U.S.C. § 1028A aggravated identity theft]

- Punishable by a term of imprisonment of not less than two years consecutive to any other sentence imposed. 18 U.S.C. §§ 1028A(a)(1) & 1028A(b)(2).

- A term of supervised release of not more than one year. 18 U.S.C. § 3583(b)(3).

- A fine not to exceed $250,000. 18 U.S.C. § 3571(b)(3).

- A mandatory special assessment of $100. 18 U.S.C. § 3013(a)(2)(A).