William D. Hyslop
United States Attorney
Eastern District of Washington
James A. Goeke
Assistant United States Attorney
Eastern District of Washington
Scott K. McCulloch
Department of Justice Trial Attorney
National Security Division
Post Office Box 1494
Spokane, Washington 99210 1494
Telephone: (509) 353 2767

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WASHINGTON

UNITED STATES OF AMERICA,

Plaintiff,

v.

LI XIAOYU (a/k/a "Oro0lxy") and [redacted]

Defendants.

4:20-CR-6019-SMJ-1

INDICTMENT

Vio.: 18 U.S.C. §§ 371, 1030(a)(2)(B), (a)(2)(C), (a)(5)(A)
Conspiracy to Access Without Authorization and Damage Computers (Count 1)

18 U.S.C. § 1832(a)(1-3), 1832(a)(5)
Conspiracy to Commit Theft of Trade Secrets (Count 2)

18 U.S.C. § 1030(a)(2)(B), (a)(2)(C), (b), (c)(2)(B)(i-iii)
Unauthorized Access to Computers (Count 3)

18 U.S.C. §§ 1349, 1343,
Conspiracy to Commit Wire Fraud (Count 4)

18 U.S.C. §§ 1028A, 2
Aggravated Identity Theft
(Counts 5-11)

Criminal Forfeiture Allegations
18 U.S.C. §§ 982(a)(2)(B),
1030(i)(1)

The Grand Jury charges:

At all times relevant to this Indictment, unless otherwise stated:

INTRODUCTION

1. Beginning no later than September 2009 and continuing until at least the date of this Indictment, together, Defendants LI XIAOYU (a/k/a "Oro0lxy") (hereinafter "LI" and/or "LI XIAOYU") and [redacted] and collectively the "Defendants," each a hacker in the People's Republic of China ("China" or "PRC"), gained unauthorized access to computers around the world and stole terabytes of data.

2. LI and [redacted] former classmates at an electrical engineering college in Chengdu, China, used their technical training to hack the computer networks of a wide variety of victims, such as companies engaged in high tech manufacturing; civil, industrial, and medical device engineering; business, educational, and gaming software development; solar energy; and pharmaceuticals. More recently, they researched vulnerabilities in the networks of biotech and other firms publicly known for work on COVID-19 vaccines, treatments, and testing technology. Their victim companies were located all across the world, including among other places the United States, Australia, Belgium, Germany, Japan, Lithuania, the Netherlands, South Korea, Spain, Sweden, and the United Kingdom.

3. The Defendants stole hundreds of millions of dollars' worth of trade secrets, intellectual property, and other valuable business information. At least once, they returned to a victim from which they had stolen valuable source code to attempt an extortion—threatening to publish on the internet, and thereby destroy the value of, the victim's intellectual property unless a ransom was paid.

4. LI and [redacted] did not just hack for themselves. While in some instances they were stealing business and other information for their own profit, in others they were stealing information of obvious interest to the PRC Government's Ministry of State Security ("MSS"). LI and [redacted] worked with, were assisted by, and operated with the acquiescence of the MSS, including MSS Officer 1, known to the Grand Jury, who was assigned to the Guangdong regional division of the MSS (the Guangdong State Security Department, "GSSD").

5. When stealing information of interest to the MSS, LI and [redacted] in most instances obtained that data through computer fraud against corporations and research institutions. For example, from victims including defense contractors in the U.S. and abroad, LI and [redacted] stole information regarding military satellite programs; military wireless networks and communications systems; high powered microwave and laser systems; a counter-chemical weapons system; and ship-to-helicopter integration systems.

6. In other instances, the Defendants provided the MSS with personal data, such as the passwords for personal email accounts belonging to individual Chinese dissidents. For example, they provided the MSS with email accounts and passwords belonging to a Hong Kong community organizer, the pastor of a Christian church in Xi'an, and a dissident and former Tiananmen Square protestor. The Defendants also stole email account contents of obvious interest to the PRC Government, such as emails between that same dissident and the office of the Dalai Lama; emails belonging to a Chinese Christian "house" (*i.e.*, not PRC

Government-approved) pastor in Chengdu, who was later arrested by the PRC government; and emails from a U.S. professor and organizer, and two Canadian residents, who advocated for freedom and democracy in Hong Kong. In some instances the Defendants reacted quickly to the PRC government's perceived desires, targeting the above-mentioned Chengdu house pastor just days after the provincial government banned his church, and conducting reconnaissance on a webmail service and a messaging app when those were used by Hong Kong citizens protesting the PRC government's recent steps to curtail freedoms there.

7. MSS Officer 1 assisted LI and other hackers. For example, when LI encountered difficulty compromising the mail server of a Burmese human rights group, MSS Officer 1 provided him with malware—a computer program designed to compromise a victim computer system—to exploit a popular internet browser. As LI had requested, MSS Officer 1 provided him "0day" malware, *i.e*. malware unknown to the software vendor and to security researchers.

8. MSS Officer 1 and other MSS officers known to the Grand Jury purported to be researchers at the "Guangdong Province International Affairs Research Center." In fact, they were intelligence officers working for the GSSD at Number 5, 6th Crossroad, Upper Nonglin Road, Yuexiu District, in Guangzhou, at the facility depicted in in these images:

//

//

//

//

//

//

//

9. The Defendants continued for years to target victims in the United States, Asia, Europe, and elsewhere from their PRC Government-provided safe-haven in China, for the benefit of the MSS and for their own personal gain.

COUNT ONE

Conspiracy to Access Without Authorization and Damage Computers, and to Threaten to Impair Confidentiality of Information

10. From at least in or about September 1, 2009, and continuing through on or about July 7, 2020, in the Eastern District of Washington and elsewhere, the Defendants did knowingly conspire and agree with each other, and with others known and unknown to the Grand Jury including officers of the MSS and MSS Officer 1, to commit offenses against the United States, namely:

OBJECTS OF THE CONSPIRACY

11. It was an object of the conspiracy for Defendants LI and [redacted] to access computers without authorization, in the Eastern District of Washington and elsewhere, and thereby to obtain information from computers of departments and agencies of the United States and protected computers, for the purpose of commercial advantage and private financial gain, and in furtherance of criminal and tortious acts in violation of the law of the United States, including 18 U.S.C. § 641, theft of government property, and 18 U.S.C. § 1832(a)(1-3) and (5), theft of trade secrets, and where the value of the information did, and would if completed, exceed $5,000, in violation of 18 U.S.C. § 1030(a)(2)(B), (a)(2)(C) and 1030(c)(2)(B)(i-iii).

12. It was a further object of the conspiracy for Defendants LI and [redacted] to knowingly cause the transmission of programs, information, codes, and commands, in the Eastern District of Washington and elsewhere, and as a result of such conduct, to cause damage without authorization to computers of departments

and agencies of the United States and protected computers, and where the offense did cause and would, if completed, have caused loss aggregating $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, and, did and would have affected a computer used by or for an entity of the United States Government in furtherance of the administration of national defense and national security, in violation of 18 U.S.C. §§ 1030(a)(5)(A) and 1030(c)(4)(B).

THE DEFENDANTS

13. Defendant LI XIAOYU was a citizen of and resident of China. LI studied Computer Application Technologies at the University of Electronic Science and Technology ("UEST") in Chengdu, China. In the conspiracy, LI primarily compromised victim networks and stole information.

14. Defendant [redacted] was a citizen of and resident of China. [redacted] studied Computer Application Technologies at the same time as LI at UEST. [redacted] primarily researched victims and potential means of exploiting them.

MANNER AND MEANS OF THE CONSPIRACY
TOOLS AND TECHNIQUES OF THE DEFENDANTS

15. The manner and means by which Defendants LI and [redacted] sought to accomplish the conspiracy included, among other things, the following:

a. Defendants researched and identified victims possessing information of interest, including trade secrets, confidential business information, information concerning defense products and programs, and personal identifying information ("PII") of victim employees, customers, and others, using various sources of information including business news websites, consulting firm websites, and a variety of search websites.

b. Defendants then gained unauthorized access to victims possessing the information sought by the conspiracy. Defendants typically stole the kinds of information with which their victims were most closely associated. That is, they stole source code from software companies; information about drugs under development, including chemical designs, from pharmaceutical firms; students' PII from an education company; and weapon designs and testing data from defense contractors.

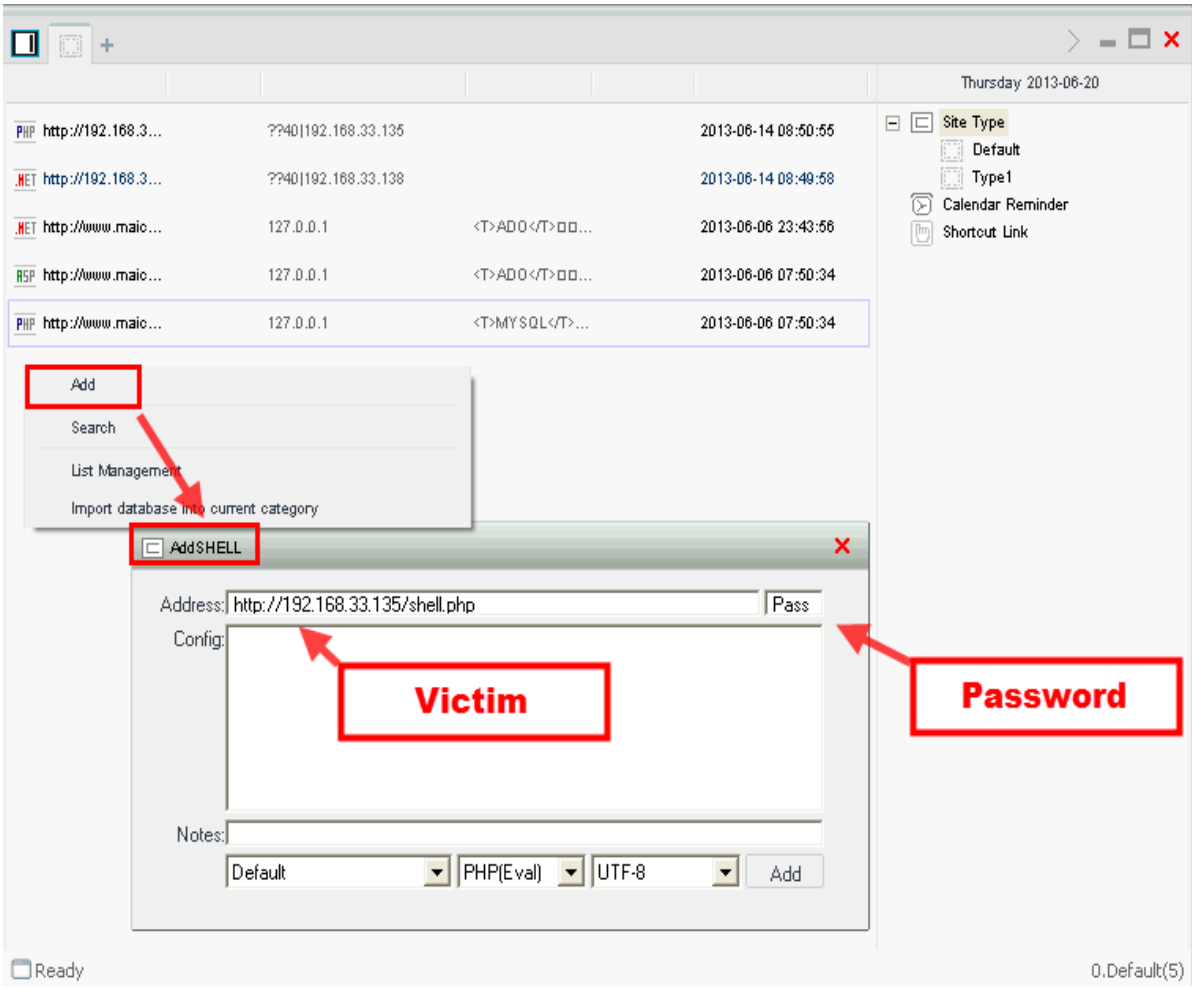
c. In some instances the Defendants targeted companies that possessed information belonging to other, partner companies—for example, the Defendants targeted a scientific research and testing company and, from it, stole information belonging to a range of that company's clients, including Victims 10 and 11.

d. The Defendants usually gained initial access to victim networks using publicly known software vulnerabilities in popular products. Those vulnerabilities were sometimes newly announced, meaning that many users would not have installed patches to correct the vulnerability. The Defendants exploited vulnerabilities in commonly used web server software, web application development suites, and software collaboration programs. They also targeted insecure default configurations in common applications.

e. The Defendants used their initial access to place malicious programs known as "web shells" on victim networks without authorization. Web shells are programs that allow the remote execution of commands on a computer.

f. The Defendants frequently employed variants of the China Chopper web shell. China Chopper is publicly available and commonly

employed by hackers working in China. It provides an easy-to-use interface through which the user can control web shells installed on multiple victim computers, as shown in this publicly-available sample image:



g. Defendants frequently disguised web shells they placed on victim networks by giving the associated files innocuous names. For example, they placed a China Chopper web shell employed against one victim under the name "p.jsp" and hid it at URL "http://[redacted].com/builds/fragments/p.jsp."

h. That, combined with the large number of China Chopper variants available, made the web shells difficult for victims to discover.

i. Defendants also sometimes secured access to their web shells with passwords.

j. In addition to web shells, Defendants frequently uploaded credential-stealing software programs to victim computer networks and then used and attempted to use the resulting stolen passwords, including passwords belonging to real, authorized network users, to gain further access to victim network.

k. Once Defendants gained access to and surveilled victim networks, they typically packaged victim data in compressed, encrypted Roshal Archive Compressed files ("RAR files").

l. The Defendants changed file names and extensions on documents and files they stole from victims computers, to make it more difficult for victims and law enforcement to identify the theft. For example, the Defendants frequently changed file names associated with the RAR files they created to extensions such as ".jpg" to make those files appear to appear to be images.

m. The Defendants frequently operated within the "recycle bin" on victim networks. The folder where recycle bin files are stored is hidden by default in the Windows operating system, and system administrators can thus be less likely to discover files saved there. Defendants often loaded malicious programs into folders they created within the recycle bin, saved RAR files they created there, and stole such files, and the data contained therein, from victim computers' recycle bins.

n. After stealing data and information from their victims and bringing that data and information back to China, Defendants then sold it for profit or provided it to the MSS, including MSS Officer 1.

o. The Defendants frequently returned to re-victimize companies, government entities, and organizations from which they had previously stolen data. In some cases the Defendants returned years after a successful data theft.

INTRUSIONS

16. During the approximate time periods identified, and from the victims whose identities are known to the Grand Jury, the defendants stole the approximate quantity and type of data as described in the table below:

U.S. VICTIMS			
Victim	**Approx. Time Frame of Activity**	**Approx. Quantity of Data Stolen**	**Nature of Data Stolen (Not Inclusive)**
Victim 1: California technology and defense firm	Dec. 2014-Jan. 2015	200 GB	Radio, laser, and antennae technology; circuit board and related algorithm designs for advanced antennae; testing mechanisms and results.
Victim 2: Maryland technology and manufacturing firm	Jan. 2015-Apr. 2015	64 GB	Testing mechanisms and results, product composition, and manufacturing processes related to high-tech materials and composites, which would reveal to competitors what products the victim was working on and allow competitors to save on research and development costs. Information related to supply chains for raw materials, such as a global shortage of a key component.

Victim 3: Hanford Site, Department of Energy, in the Eastern District of Washington ("Hanford")	Mar. 2015	<1GB	Reconnaissance information about Hanford's network and its personnel, such as lists of authorized user and administrator accounts.
Victim 4: Texas engineering and technology firm	Apr. 2015-June 2016	27 GB	Business proposals and other documents concerning space and satellite applications.
Victim 5: Virginia federal and defense contractor	Sept. 2015-Feb. 2016	140 GB	Presentations, project files, drawings, and other documents relating to projects for the U.S. Air Force and Federal Bureau of Investigation; PII belonging to more than 300 Victim 5 employees and contractors.
Victim 6: Massachusetts software firm	Mar. 2017	76 GB	Proprietary and sensitive data including software source code.
Victim 7: California software gaming company and subsidiary of a Japanese company	Mar. 2018	22 GB	Source code for two Victim 7's games, one of which had not yet been released to the public.

Victim 8: Mechanical engineering company operating in the U.S. and Japan	Apr. 2018-May 2018; Mar. 2020	1.2 TB	Proprietary and sensitive data held in the U.S. and Japan, including component engineering drawings and specifications for high-efficiency gas turbines.
Victim 9: U.S. educational software company	Nov. 2018-Feb. 2019	10 GB	Proprietary and sensitive data, including, among other things, millions of students and teachers' PII.
Victim 10: Massachusetts pharmaceutical company	Feb. 2019-Mar. 2019	2 GB	Chemical structure of anti-infective agents, the chemical engineering processes needed to create those agents, and test results from Victim 10's research, all of which would enable a competitor to focus research on areas of higher potential investment return without making the same research and development expenditures as the victim.
Victim 11: California pharmaceutical company	Feb. 2019-Mar. 2019	105 GB	Chemical structure and design of a treatment for a common chronic disease, and testing, toxicity, and dosing research related to that treatment, all of which would allow a competitor to leverage the victim's research and development expenditures.
Victim 12: Massachusetts medical device engineering company	Feb. 2019-Mar. 2019; Jan. 2020	83 GB	Source code for Victim 12's medical devices, and algorithms essential to the operation of those devices. At or about this time, the victim had partnered with a Chinese firm to produce various components for similar devices, taking care not to permit access to the victim's source code or algorithms.

Victim 13: U.S. subsidiary of a Japanese medical device and supplies company	Mar. 2019-Apr. 2019	128 GB	Proprietary and sensitive data including designs, testing data, and manufacturing plans for internal medical devices, as well as designs for machinery needed to fabricate those devices.

17. The Defendants targeted victims around the world. They tended to target companies in countries with successful technology industries. As when targeting U.S. victims, the Defendants stole data associated with the knowledge areas for which those overseas victims were best known. The Defendants' overseas victims included, among others:

OVERSEAS VICTIMS		
Victim	**Approx. Time Frame of Activity**	**Defendant Conduct**
Victim 14: Large electronics firm in the Netherlands	Feb. 2016	Compromised Victim 14's computer network.
Victim 15: Swedish online gaming company	Mar. 2017	Stole approximately 169 gigabytes of data concerning, among other things, development build code for Victim 15's products; developer keys and certificates; usernames and passwords; and code associated with in-game upgrades.
Victim 16: Lithuanian gaming company	Apr. 2017	Stole approximately 38 gigabytes of data concerning, among other things, programming data, Java files, and encoding files.

Victim 17: German construction software company	May 2017	Stole approximately 1 GB of, among other things, source code for Victim 17's products.
Victim 18: German software engineering firm	Apr. 2017	Stole approximately 2 gigabytes of data from company that creates products designed to manage, among other things, wireless networks and Internet of Things ("IoT") platforms.
Victim 19: Belgian engineering software company	Mar. 2018-Apr. 2018	Stole approximately 142 gigabytes of documents including, among other things, source code for Victim 19's products, imaging tools, and algorithms, associated with computational fluid dynamics.
Victim 20: Civil and transportation engineering firm in the Netherlands	Feb. 2019-July 2019	Compromised Victim 20's computer network.
Victim 21: Australian defense contractor	Apr. 2019-June 2019	Stole approximately 320 gigabytes of documents including, among other things, source code for Victim 21's products; engineering schematics; and technical manuals.
Victim 22: South Korean shipbuilding and engineering firm	June 2019-July 2019	Stole approximately 842 megabytes of documents concerning, including, among other things, IoT software and smart factory development.

Victim 23: Australian solar energy engineering concern	Jan. 2020	Compromised Victim 23's network and conducted additional network reconnaissance.
Victim 24: Spanish electronics and defense firm	Mar. 2020	Stole approximately 900 GB of documents from a company that engineers technology solutions in civilian and defense sectors.
Victim 25: U.K. artificial intelligence and cancer research firm	Apr. 2020	Compromised the network of Victim 25.

18. These numbered victims represent only a small percentage of the Defendants' offense conduct. The Defendants and their co-conspirators compromised hundreds of victims.

OVERT ACTS

19. In furtherance of the conspiracy, and to affect its unlawful objects, LI and [redacted] committed and caused to be committed the following overt acts, among others, in the Eastern District of Washington and elsewhere.

20. On or about December 3, 2014, LI conducted reconnaissance on a U.S. Navy contracting portal containing information about companies including Victim 5.

21. On or about December 26 and 30, 2014, [redacted] conducted reconnaissance on Victim 5 by a variety of means, including viewing data about the company that was available on the website of a consulting firm.

22. On or about December 4, 2015, LI accessed a China Chopper web shell program on Victim 5's network at "[redacted].com/irj/api.jsp."

23. On or about December 4, 2015, LI used a Victim 5's employee's credentials without authorization and obtained information that the employee was authorized to access.

24. On or about August 10, 2019, LI attempted but failed to again access Victim 5's network, using the usernames and passwords of three company personnel.

25. In or about December 2014, LI compressed Victim 1's files into RAR files, divided those RAR files into smaller sub-files, and then removed the RAR files.

26. On or about December 29, 2014, [redacted] accessed Victim 1's stolen RAR files.

27. On or about January 16, 2015, LI conducted reconnaissance on Victim 2's network, including scanning IP addresses associated with the network, attempting to access network administrator tools, and browsing subdomains.

28. During the Victim 2 intrusion, LI saved a Javascript, password-protected web shell to Victim 2's network under filename chengshu_jsp.java.

29. On or about April 25, 2015, LI transferred files stolen from Victim 2's network to China.

30. On or about August 5, 2019, LI attempted unsuccessfully to regain unauthorized access to Victim 2's network.

31. In or around March 2015, LI accessed a web shell program named "lm.aspx" on the Hanford computer network.

32. LI also hid another web shell from Hanford's network defenders, naming the other "toolbars.cfm," and password protecting it.

33. On or about March 16, 2015, LI used a web shell to execute command "whoami" (to list the username of the account that he was using to run commands) on Hanford's network.

34. That same day, LI used a web shell to execute command "net localgroup administrators" on Hanford's network, to print the list of user accounts possessing administrator-level privileges.

35. On or about November 15, 2018, LI attempted to exploit an Adobe ColdFusion vulnerability that had been publicly identified and patched in September 2018 (9 CVE-2018-15961) by navigating to the file manager on Hanford's network associated with text editing program CKEditor, at [redacted]ckeditor/plugins/-filemanger/filemanager.cfm.

36. The Defendants failed to access this CKEditor file manager. But Hanford was not the only entity Defendants sought to exploit using CVE-2018-15961.

a. On or about October 20, 2018, LI navigated to the network of another victim—a U.S. government biomedical research agency in Maryland.

b. There, too, LI navigated to the file manager at [redacted]ckeditor/-plugins/filemanager/filemanager.cfm. LI successfully accessed the file manager.

c. Then, he used that access to upload a ColdFusion web shell program named "cfm backdoor by ufo" to the ckeditor file manager.

d. One minute later, he used that ColdFusion web shell to upload another, China Chopper web shell to the victim's network.

37. In or around April 2015, [redacted] conducted reconnaissance on U.S. engineering and technology companies, including Victim 4.

38. In the course of that reconnaissance, [redacted] employed a third-party network research tool to analyze Victim 4's computer network.

39. On or about June 15 and 16, 2016, LI compressed and encrypted Victim 4's documents into RAR files falsely labeled with ".jpg" file extensions to mimic image files.

40. On or about February 29, 2016, LI accessed a web shell on Victim 14's network at http://origin.www.[redacted].com/Q2O/CFIDE/-scripts/error.cfm.

41. On or about March 16, 2017, LI used a China Chopper web shell to change the last-modified time of Victim 15's files (a technique known as "timestomping").

42. On or about April 21, 2017, LI compromised Victim 18's network by exploiting a vulnerability in web application development software running on Victim 18's server.

43. On or about April 29, 2017, LI compressed a Victim 16's network directory into a "tarball," a compressed file format in the Linux operating system.

44. On or about May 22, 2017, LI downloaded a RAR file from Victim 17's network, and transferred it to China.

45. LI emailed several Victim 6's personnel on or about December 6, 2017, with the subject line "Source Code To Be Leaked!"

a. LI emailed them using a compromised mail server and an email account hosted on the network of another company.

b. In his email, LI demanded Victim 6 pay $15,000 in cryptocurrency.

c. In that same email, LI threatened to "publish all [Victim 6's] source code" to the internet unless he was paid.

d. LI also attached a file containing a folder named "demo pro e source code" to his email, containing source code stolen from Victim 6 in or around March 2017.

46. On or about March 8, 2018, LI downloaded three RAR files with ".jpg" file extensions from Victim 7's network.

47. On or about March 21, 2018, LI accessed a China Chopper web shell he had placed on the network of Victim 19, at http://helpdesk.[redacted].be/-uuid/HttpServletWrapper.

48. On or about April 30, 2018, LI used stolen, valid credentials to access Victim 8's mail server in Tokyo, Japan.

49. On or about March 10, 2020, LI used stolen, valid system account credentials to access Victim 8's webmail server.

50. On or about December 1, 2018, LI transferred 649 megabytes of data stolen from Victim 9 to China.

51. On or about December 2, 2018, LI transferred 9.5 gigabytes of data stolen from Victim 9 to China.

52. On or about February 27, 2019, LI accessed Victim 12's network via a China Chopper web shell at URL http://[redacted].com/custom/login/tst.jsp.

53. On or about the same day, LI accessed Victim 12's web server using stolen, valid credentials.

54. On or about May 11, 2020, LI navigated to the same URL at which he had placed the web shell on Victim 12's network, but the web shell was no longer present.

55. On or about March 17, 2019, LI logged in to a Chinese, invitation-only criminal hacking forum.

56. On or about February 7, 2019, LI accessed a China Chopper web shell he had placed on the network of Victim 20, at http://[redacted].com/SQLTrace-/i.jsp.

57. On or about March 21, 2019, LI used the valid credentials of a Victim 13 network user to create a subfolder within Victim 13's network recycle bin, and then created RAR files containing Victim 13's data in the recycle bin.

58. On or about April 18, 2019, LI accessed a China Chopper web shell on Victim 21's network at http://confluence.[redacted].com/i.jsp.

59. On or about June 26, 2019, LI timestomped Victim 22's files to disguise his actions on Victim 22's network.

60. On or about January 25 and 27, 2020, LI searched for vulnerabilities at a Maryland biotech firm. That firm had announced less than a week earlier that it was researching a potential COVID-19 vaccine.

61. On or about January 27, 2020, LI conducted reconnaissance on the computer network of a Massachusetts biotech firm publicly known to be researching a potential COVID-19 vaccine.

62. On or about January 28, 2020, LI accessed Victim 23's network via a China Chopper web shell.

63. LI then executed commands on Victim 23's network that enabled him to view reconnaissance information such as directory contents and user privileges.

64. On or about February 1, 2020, LI searched for vulnerabilities in the network of a California biotech firm that had announced one day earlier that it was researching antiviral drugs to treat COVID-19.

65. On or about March 17, 2020, LI accessed Victim 24's network and browsed 40 RAR files, named with ".jpg" image-file extensions, in folder webmail.[redacted].es/aspnet_client/images/.

66. On or about April 1, 2020, LI accessed a China Chopper web shell on Victim 25's network at [redacted].com/confluence/plugins/-servlet/URA.

67. On or about May 12, 2020, LI searched for vulnerabilities in the network of a California diagnostics company that is publicly known to be involved in the development of COVID-19 testing kits.

68. On or about June 13, 2020, LI conducted reconnaissance on the network of a Virginia defense and cybersecurity contractor.

69. On or about June 13, 2020, LI conducted reconnaissance on Hong Kong protestor communication methods.

70. On or about June 13, 2020, LI conducted reconnaissance on the network of Hong Kong webmail provider Netvigator.

71. On or about June 13, 2020, LI conducted reconnaissance on a U.K. messaging application frequently used by Hong Kong protestors.

72. On or about June 13, 2020, LI conducted reconnaissance on the network of a Massachusetts biotech firm focused on cancer treatment.

73. On or about June 13, 2020, LI searched for vulnerabilities in the network of a California space flight and aerospace engineering firm.

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

COUNT TWO

Conspiracy to Commit Theft of Trade Secrets

74. The allegations contained in paragraphs 1 through 9 and 13 through 73 are realleged and incorporated as if set forth herein.

75. From at least on or about September 1, 2009, until on or about July 7, 2020, Defendants LI and [redacted], intending to convert trade secrets to the economic benefit of someone other than their owners, and intending and knowing that the offense would injure such owners, conspired with each other and with others known and unknown to the Grand Jury to:

a. Knowingly and without authorization steal, appropriate, take, and by fraud, artifice, and deception obtain trade secrets that were related to a product or service used in and intended to be used in interstate and foreign commerce;

b. Knowingly and without authorization copy, duplicate, alter, replicate, transmit, deliver, send, communicate, and convey trade secrets that were related to a product or service used in and intended to be used in interstate and foreign commerce; and

c. Knowingly receive, buy, and possess trade secrets that were related to a product or service used in and intended to be used in interstate and foreign commerce, knowing the same to have been stolen, appropriated, obtained, and converted without authorization.

76. LI and [redacted] conspired to steal trade secret information from Victim 1, Victim 2, Victim 6, Victim 7, Victim 10, Victim 11, Victim 12, and Victim 13. Each of the victims took reasonable measures to keep this information secret, and such information derived independent economic value from not being generally known, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.

77. In furtherance of the conspiracy, and to effect the purpose and objects thereof, Defendants LI and [redacted], and others, committed various overt acts in the Eastern District of Washington and elsewhere, including, but not limited to, the overt acts identified in paragraphs 25 through 30, 45 through 46, 52 through 54, and 57, in violation of 18 U.S.C. §§ 1832(a)(1-3), all in violation of 18 U.S.C. §§ 1832(a)(5).

COUNT THREE

Computer Fraud and Abuse: Unauthorized Access

78. The allegations contained in paragraphs 1 through 9 and 13 through 73 are realleged and incorporated as if set forth herein.

79. In or about November 2018, in the Eastern District of Washington and elsewhere, Defendants LI and [redacted] aided and abetted by each other and others known and unknown to the Grand Jury, attempted to access and accessed computers of the United States, specifically the Department of Energy, and protected computers, in the Eastern District of Washington, without authorization to obtain information, in furtherance of violations of the United States, including, inter alia, 18 U.S.C. § 641, all in violation of 18 U.S.C. §§ 1030(a)(2)(B), (a)(2)(C), (b), and (c)(2)(B)(i-iii).

COUNT FOUR

Conspiracy to Commit Wire Fraud

80. The allegations contained in paragraphs 1 through 9 and 13 through 73 are realleged and incorporated as if set forth herein.

81. From at least on or about September 1, 2009, until on or about July 7, 2020, in the Eastern District of Washington and elsewhere, the Defendants, LI and [redacted] did knowingly and intentionally conspire with each other and others known and unknown to the Grand Jury, including officers of the MSS including MSS Officer 1, to devise a scheme and artifice to defraud and to obtain property from the United States and others, by means of materially false and fraudulent pretenses, representations and promises—including among others the presentation of false identification to gain unauthorized access to computers—and did knowingly transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds, namely malicious code, for the purpose of executing and attempting to execute

such scheme and artifice, in violation of 18 U.S.C. § 1343, all in violation of 18 U.S.C. § 1349.

COUNTS FIVE through ELEVEN

Aggravated Identity Theft

82. The allegations contained in paragraphs 1 through 73 and 78 through 81 are realleged and incorporated as if set forth herein.

83. On or about the dates set forth below, in the Eastern District of Washington and elsewhere, the Defendants, LI and [redacted] aided and abetted by each other and by others known and unknown to the Grand Jury, during and in relation to the crime of Unauthorized Access to Computers, in violation of 18 U.S.C. § 1030(a)(2)(B), (a)(2)(C), (b), (c)(2)(B)(i-iii) and the crime of Conspiracy to Commit Wire Fraud, in violation of 18 U.S.C. §§ 1343 and 1349, did knowingly transfer, possess, and use, without lawful authority, the means of identification of another person:

COUNT	ON OR ABOUT	IDENTIFICATION OF ANOTHER PERSON
Five	December 4, 2015	LI accessed the network of Victim 5 using username dj*** and that real user's password.
Six	March 16, 2017	LI accessed the network of Victim 6 with username rg****** and that real user's password.
Seven	March 26, 2017	LI accessed the network of Victim 6 with username kh********** and that real user's password.
Eight	February 26, 2019	LI stole and possessed two usernames and associated passwords associated with real users from Victim 12.

Nine	March 21, 2019	LI stole and possessed four usernames and associated passwords associated with real users from Victim 13.
Ten	March 21, 2019	LI accessed the network of Victim 13 with username ke********** and that real user's password.
Eleven	August 10, 2019	LI attempted to access the network of Victim 5 using three Victim 5 usernames and associated passwords all associated with real users.

All in violation of 18 U.S.C. §§ 1028A and 2.

CRIMINAL FORFEITURE ALLEGATIONS

84. As a result of committing one or more of the offenses alleged in Counts One through Eleven of this Indictment, Defendants LI and [redacted] shall forfeit to the United States, pursuant to 18 U.S.C. §§ 982(a)(2)(B) and 1030(i)(1), the Defendants' interests in any personal property that was used or intended to be used to commit or facilitate the commission of such offenses, and any property constituting, or derived from, proceeds obtained directly or indirectly as a result of one or both of the said offenses, including but not limited to the sum of money representing the amount of proceeds obtained as a result of one or both of the said offenses.

85. If any one of the above-described forfeitable property, 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 person;

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 subdivided without difficulty;

it is the intent of the United States, pursuant to 18 U.S.C. § 982(b)(1) and 21 U.S.C. § 853(p), to seek forfeiture of any other property of said defendants up to the value of the above forfeitable property.

DATED this ___day of July, 2020.

A TRUE BILL

Foreperson

_____
William D. Hyslop
United States Attorney

_____
James A. Goeke
Assistant United States Attorney

_____
Scott K. McCulloch
Department of Justice Trial Attorney
National Security Division