

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

v.

WU HAIBO,

a/k/a "shutd0wn,"

a/k/a "Boss Wu,"

a/k/a "吴海波,"

CHEN CHENG,

a/k/a "lengmo,"

a/k/a "Chief C,"

a/k/a "Jesse Chen,"

a/k/a "陈诚,"

LIANG GUODONG,

a/k/a "梁国栋"

MA LI,

a/k/a "Mary,"

a/k/a "马丽,"

WANG YAN,

a/k/a "crysolo,"

a/k/a "王堰,"

WANG ZHE,

a/k/a "ken73224,"

a/k/a "王哲,"

ZHOU WEIWEI,

a/k/a "nullroot,"

a/k/a "周伟伟,"

XU LIANG,

a/k/a "徐梁,"

WANG LIYU,

a/k/a "PICNIC350116,"

a/k/a "王立宇,"

SHENG JING,

a/k/a "sjbible,"

a/k/a "盛晶,"

Defendants.

SEALED INDICTMENT

24 Cr. ____ (____)

24 CRIM 687

COUNT ONE
(Conspiracy to Commit Computer Intrusions)

The Grand Jury charges:

Overview

At all times relevant to this Indictment:

1. The People’s Republic of China’s (“PRC”) Ministry of State Security (“MSS”) had responsibility for the PRC’s domestic counterintelligence, non-military foreign intelligence, and aspects of the PRC’s political and domestic security. The PRC’s Ministry of Public Security (“MPS”) had responsibility for the PRC’s public and political security, including responsibility for law enforcement. To acquire information of interest to the PRC government in a manner that obscured their involvement, the PRC’s MSS and MPS used an extensive network of private companies and contractors in China to conduct unauthorized computer intrusions (“hacks”) in the United States and elsewhere.

2. From at least in or around 2016 through in or around 2023, in the Southern District of New York and elsewhere, the Chinese technology company Anxun (i-Soon) Information Technology Co., Ltd., a/k/a 安洵信息技术有限公司, a/k/a “i-Soon” (“i-Soon”), and its personnel, engaged in the numerous and widespread hacking of email accounts, cell phones, servers, and websites at the direction of, and in close coordination with, the PRC’s MSS and MPS. Incorporated in or around 2010 in Shanghai, China, i-Soon profited and grew as a key player in the PRC’s hacker-for-hire ecosystem. In or around 2021, i-Soon generated tens of million dollars in revenue and its executives estimated that its revenues would reach approximately \$75 million by 2025. At certain times, i-Soon had over 100 employees.

3. i-Soon employees hacked and attempted to hack victims across the globe, including a large religious organization in the United States, critics and dissidents of the PRC government,

a state legislative body, United States government agencies, the ministries of foreign affairs of multiple governments in Asia, and news organizations. i-Soon's victims were of interest to the PRC government because, among other reasons, they were prominent overseas critics of the PRC government or because the PRC government considered them threatening to the rule of the Chinese Communist Party.

i-Soon's Relationship with the MSS and MPS

4. i-Soon's primary customers were PRC government agencies, including the MSS and the MPS. i-Soon worked with at least 43 different MSS or MPS bureaus in at least 31 separate provinces and municipalities in China. These bureaus sometimes operate independently of one another, and i-Soon cultivated relationships with and sold its products to multiple bureaus.

5. A core part of i-Soon's business was conducting hacking to steal data on behalf of the PRC government, including the MSS and the MPS. i-Soon charged the MSS and MPS equivalent to between approximately \$10,000 and \$75,000 for each email inbox it successfully hacked. i-Soon also offered analysis of the contents of stolen data, and it charged the MSS and MPS additional fees for that analysis.

6. In some instances, i-Soon conducted its hacking at the direct request of the MSS or MPS. In other instances, i-Soon conducted hacks on its own initiative and then sold, or attempted to sell, the stolen data to different bureaus of the MSS or MPS. i-Soon also trained MPS employees how to hack independently of i-Soon.

Means and Methods of the Conspiracy

7. i-Soon used different methods to hack into computer systems—and offered many of these methods for sale to its customers. i-Soon touted what it called a “industry-leading offensive and defensive technology” and a “zero-day vulnerability arsenal” used to successfully

hack computer systems. A “zero-day” is a vulnerability in a computer system that is unknown to its owners or anyone capable of mitigating it.

8. One way i-Soon accomplished its hacks was through “spear phishing” emails. In a typical i-Soon spear phishing campaign, a malicious actor sends an email or other online message to a victim, which message attempts to trick the victim into either clicking a link that will download malicious software (“malware”) onto the victim’s computer or unwittingly providing account credentials (*i.e.*, username and password) to the malicious actor.

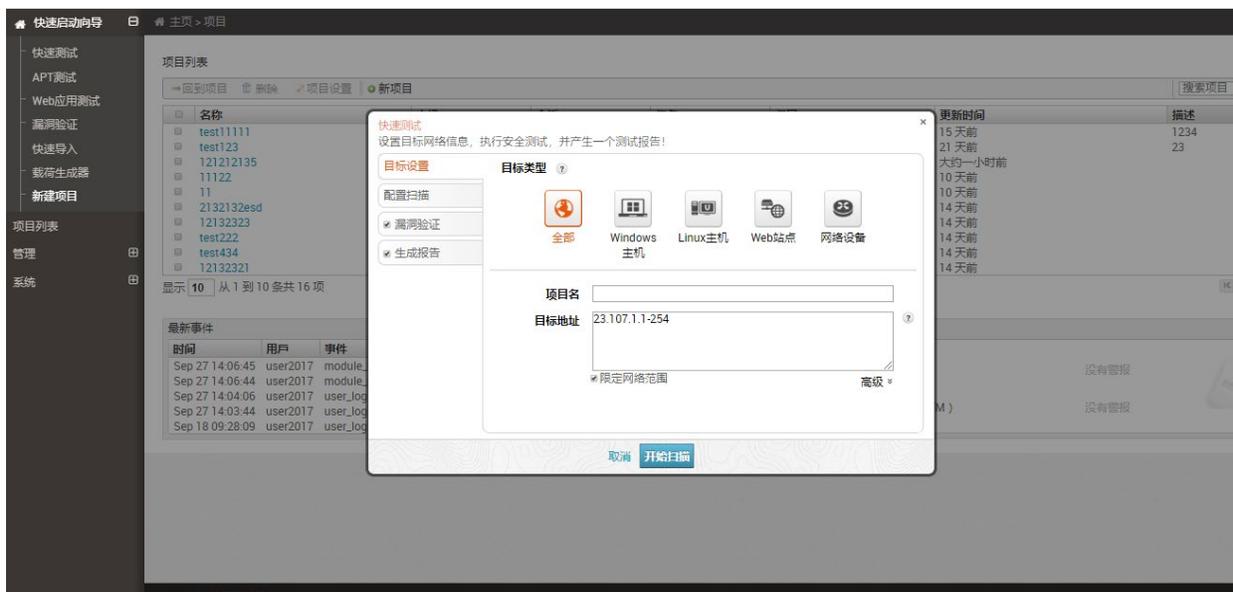
9. i-Soon developed a list of “rules” for its employees to keep in mind when spear phishing. The “rules” were designed to help i-Soon’s employees trick i-Soon’s victims into providing access to computer systems. For example, the first rule stated, “No batch sending, no batch sending, no batch sending.” Spear phishing emails are easier to detect as malicious if they are sent repeatedly.

10. The second rule emphasized social engineering by stating, “Don’t send an interface link in the first email. Send an interface link after email chats. Please refer to the provided successful cases.” Similarly, the seventh rule stated, “Strategy is very important. The purpose should not be so obvious. Must chat with the target first before giving the link.” Spear phishing attacks are often more effective when they are supported by additional social engineering, which involves manipulating, influencing, or deceiving a victim in order to gain control over a computer system, or to steal personal and financial information.

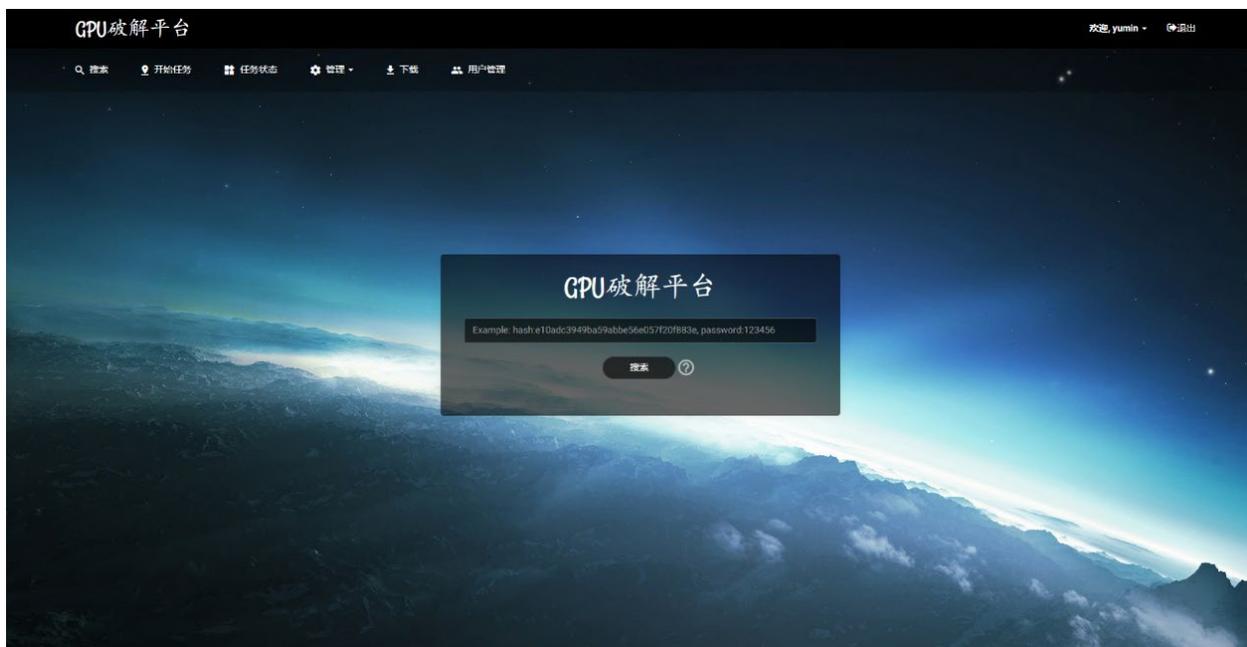
11. i-Soon internal documents described its hacking as “penetration testing” and assigned employees to that task. “Penetration testing” refers to an authorized cyberattack on a computer system to test its security. i-Soon’s activity was not, in fact, true penetration testing, because i-Soon’s hacking activity was unauthorized by the end target.

12. i-Soon offered for sale platforms that the MSS and the MPS employees could use to hack on their own. For example:

a. One of i-Soon’s products was software called the “Automated Penetration Testing Platform.” i-Soon advertised the platform’s ability to send email phishing attacks, to create files with malware that could provide access to victims’ computers if opened, and to clone websites of victims in order to induce them to submit personal information. An image of the interface for the Automated Penetration Testing Platform is below:



b. Another of i-Soon’s products was software that allowed the user to gain unauthorized access to online accounts or computer systems by deciphering passwords—also called “password cracking.” This platform was called the “Divine Mathematician Password Cracking Platform.” An image of the interface for the Divine Mathematician Password Cracking Platform is below:



c. Yet other of i-Soon's products were software specifically designed to target victim accounts on a variety of computer systems and applications, including Microsoft Outlook; Gmail, the email service provided by Google LLC; the social media network X, formerly known as Twitter; the cellphone operating system Android; and the computer operating systems Windows, Macintosh, and Linux. i-Soon advertised its bespoke software as being able to overcome the unique defenses of these systems.

d. For example, as to Outlook, i-Soon sold software with the ability to generate a spear phishing link and then to download the content of a victim's Outlook mailbox if the victim clicked the link. i-Soon's platform was further able to bypass multi-factor authentication in some cases and could manage access to multiple victim accounts at once. An image of the interface for i-Soon's Outlook platform is below:

The screenshot shows the 'Outlook邮件取证平台' (Outlook Mail Platform) interface. The top navigation bar includes 'Outlook邮件取证平台', a search icon, '重新登录', and '退出'. The left sidebar contains a user profile for 'adminadmin' with login and authorization details, and a menu with options: '首页', '取证成功列表', '下载列表', '系统配置', '操作日志', and '用户管理'. The main content area displays a table with 9 rows of email account data.

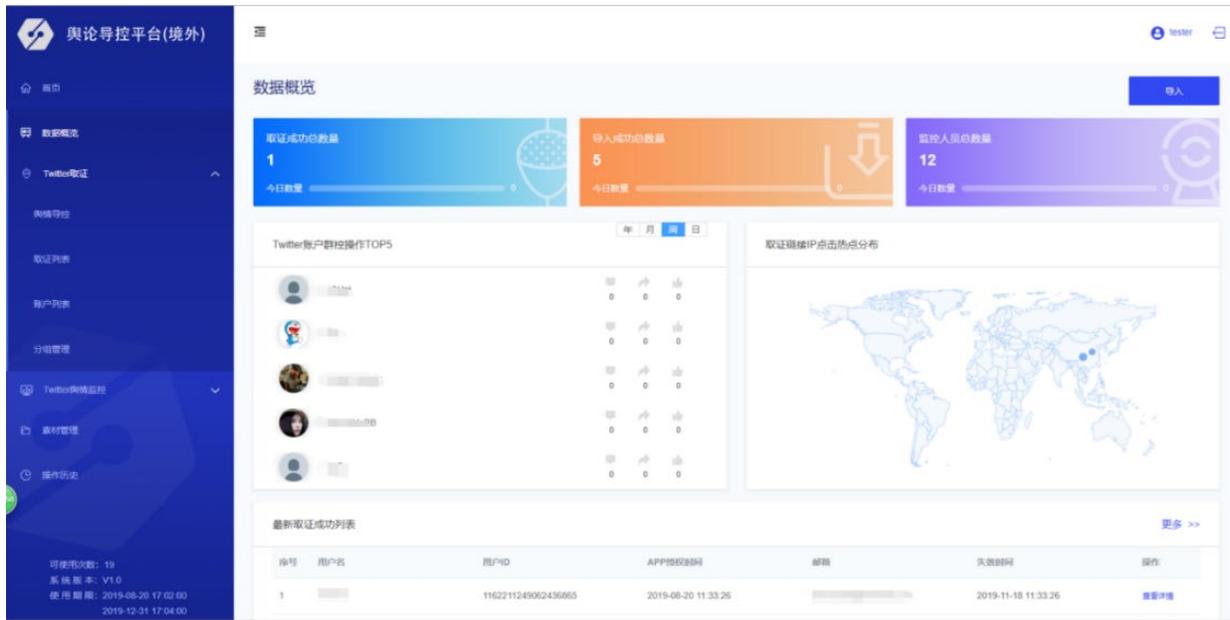
序号	邮箱	起止时间	收取邮件时间	密码	进度	操作
1	[redacted]@hotmail.com	[2018-09-01] --> [2018-09-28]	2018-09-27 14:57:59	QNLZyGc5	100%	[download] [delete]
2	[redacted]@outlook.com	[2018-08-26] --> [2018-09-25]	2018-09-25 16:24:14	Jl5grRTU	100%	[download] [delete]
3	[redacted]@outlook.com	[2018-08-26] --> [2018-09-25]	2018-09-25 16:08:35	CePLoDoA	100%	[download] [delete]
4	[redacted]@outlook.com	[2018-08-26] --> [2018-09-25]	2018-09-25 15:36:00	NyLcRn2p	100%	[download] [delete]
5	[redacted]@outlook.com	[2018-08-01] --> [2018-09-25]	2018-09-25 13:41:59	BXrYncxh	100%	[download] [delete]
6	[redacted]@outlook.com	[2018-08-01] --> [2018-08-31]	2018-09-25 11:32:11	2o6yV89a	100%	[download] [delete]
7	[redacted]@hotmail.com	[2018-07-01] --> [2018-08-31]	2018-09-25 11:30:54	Stx3mY0w	100%	[download] [delete]
8	[redacted]@outlook.com	[2018-09-01] --> [2018-09-21]	2018-09-21 11:52:16	IVBW7kz9	100%	[download] [delete]
9	[redacted]@hotmail.com	[2018-09-01] --> [2018-09-21]	2018-09-21 11:52:07	HGuSImj0	100%	[download] [delete]

e. As another example, with respect to Gmail, i-Soon sold software with the capability to send a victim a spear phishing link and then to obtain access to and control over the victim's Gmail account. The software had the capability to download the contents of a victim's Gmail account, including messages in the victim's inbox, messages previously sent by the victim, and draft emails saved in the victim's account. Once it gained access to a Gmail account, i-Soon's software was able to bypass multi-factor authentication defenses. An image of the interface for i-Soon's Gmail platform is below:



f. As another example, with respect to Twitter, i-Soon sold software with the capability to send a victim a spear phishing link and then to obtain access to and control over the victim’s Twitter account. The software had the ability to access Twitter even without the victim’s password and to bypass multi-factor authentication. After a victim’s Twitter was compromised, the software could send tweets, delete tweets, forward tweets, make comments, and like tweets. The purpose of this software was to help i-Soon’s customers, including the PRC government, use hacked Twitter accounts to understand public opinion outside of China. For example, the software could be set to keep track of keywords appearing in tweets or messages. i-Soon referred to this software as its “Public Opinion Guidance and Control Platform (Overseas).”¹ An image from the “Public Opinion Guidance and Control Platform (Overseas)” is below:

¹ See language at top left of image.



The i-Soon Defendants

13. During certain periods relevant to the crimes charged in this Indictment, WU HAIBO, a/k/a “shutd0wn,” a/k/a “Boss Wu,” a/k/a “吴海波,” CHEN CHENG, a/k/a “lengmo,” a/k/a “Chief C,” a/k/a “Jesse Chen,” a/k/a “陈诚,” LIANG GUODONG, a/k/a “梁国栋,” MA LI, a/k/a “马丽,” WANG YAN, a/k/a “crysolo,” a/k/a “王堰,” WANG ZHE, a/k/a “ken73224,” a/k/a “王哲,” ZHOU WEIWEI, a/k/a “nullroot,” a/k/a “周伟伟,” XU LIANG, a/k/a “徐梁,” the defendants, worked for i-Soon, and had the following roles in the conspiracy:

a. WU HAIBO, a/k/a “shutd0wn,” a/k/a “Boss Wu,” a/k/a “吴海波,” the defendant, was the Chief Executive Officer, and leader, of i-Soon. WU oversaw and directed i-Soon’s hacking operations. WU also took overt acts in furtherance of the conspiracy to commit computer intrusions. For example, WU acquired a domain used in connection with i-Soon’s hacking operations.

b. CHEN CHENG, a/k/a “lengmo,” a/k/a “Chief C,” a/k/a “Jesse Chen,” a/k/a “陈诚,” the defendant, was the Chief Operating Officer of i-Soon. CHEN ran many of i-Soon’s

operations, including support of its hacking operations. CHEN tasked other employees of i-Soon with carrying out hacks, made executive decisions about how and if hacks would be carried out, and coordinated with the MPS and the MSS employees about selling data stolen from victims.

c. MA LI, a/k/a “马丽,” the defendant, was the leader of the “Infrastructure Support Team” of i-Soon. MA conducted operations, including hacking operations, for i-Soon. MA carried out some of i-Soon’s hacks herself, assisted other i-Soon employees with their hacking activity, and coordinated with other i-Soon employees, including executive CHEN, about the progress or results of hacking operations.

d. WANG YAN, a/k/a “crysolo,” a/k/a “王堰,” the defendant, was the leader of one of i-Soon’s “penetration testing” teams. WANG hacked computer systems for i-Soon. He also tasked other i-Soon employees with carrying out hacking operations and coordinated with other i-Soon employees about the progress and results of hacks.

e. LIANG GUODONG, a/k/a “梁国栋,” the defendant, was an employee of i-Soon. LIANG hacked computer systems for i-Soon and acquired infrastructure for i-Soon’s hacking operations.

f. WANG ZHE, a/k/a “ken73224,” a/k/a “王哲,” the defendant, was the Sales Director of i-Soon. WANG sold i-Soon’s cyberattack products and capabilities, as well as information i-Soon obtained from its hacking operations.

g. ZHOU WEIWEI, a/k/a “nullroot,” a/k/a “周伟伟,” the defendant, was the leader of i-Soon’s “Technology Research and Development Center.” ZHOU supported the targeting and hacking operations of other i-Soon employees.

h. XU LIANG, a/k/a “徐梁,” the defendant, was a “penetration tester” for i-Soon. XU carried out some of i-Soon’s hacking operations. For example, in or around December 2016, XU

initiated a Distributed Denial of Service (“DDoS”) attack against the website that published information critical of the Chinese Communist Party, identified below as Newspaper-1. A DDoS attack overwhelms a target website with a flood of internet traffic. As another example, in or around August 2017, XU attempted a DDoS attack against a website at the direction of the MPS.

The MPS Defendants

14. During certain periods relevant to the crimes charged in this Indictment, WANG LIYU, a/k/a “PICNIC350116,” a/k/a “王立宇,” and SHENG JING, a/k/a “sjbible,” “盛晶,” the defendants, worked for the MPS, and had the following roles in the conspiracy:

a. WANG LIYU, a/k/a “PICNIC350116,” a/k/a “王立宇,” the defendant, was an MPS officer based in Chengdu, China. WANG tasked i-Soon with hacking specific targets, including a U.S. news organization perceived as critical of the PRC government, and purchased data that i-Soon had stolen from victims’ computer systems.

b. SHENG JING, a/k/a “sjbible,” “盛晶,” the defendant, was an MPS officer based in Shenzhen, China. SHENG tasked i-Soon with hacking specific targets, including a Chinese dissident residing in the United States and a U.S. news organization perceived as critical of the PRC government, and received information from i-Soon stolen from victims’ computer systems, including a religious leader.

i-Soon’s Campaign of Cyber Attacks in the United States

15. Between in or around 2016 and in or around 2023, i-Soon employees hacked or attempted to hack a series of victims in the United States. Some of these hacks were at the direction of the MSS or the MPS, or the results of the hacks were provided to the MSS or the MPS. i-Soon’s targets in the United States included a large religious organization, critics and dissidents of the

PRC government, a state legislative body, United States government agencies, and news organizations.

16. i-Soon employees understood that their hacking could result in U.S. sanctions and criminal charges.

Attack on Newspaper-1

17. Newspaper-1 is a publication based in New York, New York, that publishes news related to China and is opposed to the Chinese Communist Party.

18. In or around December 2016, at the direction of WANG LIYU, a/k/a “PICNIC350116,” a/k/a “王立宇,” the defendant, an officer of the Chengdu MPS, i-Soon employees successfully launched a DDoS attack against Newspaper-1’s website. i-Soon’s attack temporarily shut down Newspaper-1’s website.

19. In or around May 2017, i-Soon successfully compromised a number of email accounts belonging to executives and writers of Newspaper-1. Specifically, by on or about May 9, 2017, LIANG GUODONG, a/k/a “梁国栋,” the defendant, an i-Soon employee, had successfully exfiltrated emails from Newspaper-1’s Chief Editor and a vice president. In addition, on or about May 5, 2017, WANG LIYU, a/k/a “PICNIC350116,” a/k/a “王立宇,” the defendant, provided i-Soon with the username and password of the administrator account for Newspaper-1’s website.

20. In or around September 2017, at the direction of MPS officer SHENG JING, a/k/a “sjbible,” a/k/a “盛晶,” the defendant, i-Soon identified Internet Protocol (“IP”) addresses within China that had accessed the website of Newspaper-1 in an attempt to assist the MPS in locating dissidents located in China. An IP address is a numerical label assigned to a particular device connected to the Internet. i-Soon had obtained the IP address information from its earlier breach

of Newspaper-1's website, and i-Soon sold the MPS a spreadsheet identifying IP addresses that had accessed the website of Newspaper-1 from within China.

Attack on Individual-1

21. Individual-1 resided in the United States and held himself out as an opponent of the PRC government.

22. Between 2017 and 2019, at the direction of the MPS, including WANG LIYU, a/k/a "PICNIC350116," a/k/a "王立宇," and SHENG JING, a/k/a "sjbible," a/k/a "盛晶," the defendants, i-Soon employees, including CHEN CHENG, a/k/a "lengmo," a/k/a "Chief C," a/k/a "Jesse Chen," a/k/a "陈诚," WU HAIBO, a/k/a "shutd0wn," a/k/a "Boss Wu," a/k/a "吴海波," LIANG GUODONG, , a/k/a "梁国栋," XU LIANG, a/k/a "徐梁," and WANG YAN, a/k/a "crysolo," a/k/a "王堰," the defendants, repeatedly targeted and successfully compromised accounts controlled by Individual-1 and his associates at the direction of the MPS.

Attack on the Defense Intelligence Agency

23. The United States Defense Intelligence Agency (the "DIA") is an agency within the Department of Defense that specializes in defense and military intelligence.

24. In or around October 2017, i-Soon employees, including WU HAIBO, a/k/a "shutd0wn," a/k/a "Boss Wu," a/k/a "吴海波," and LIANG GUODONG, a/k/a "梁国栋," the defendants, attempted to obtain access to the email inboxes of DIA employees by sending spear phishing emails to more than one hundred DIA email accounts. The spear phishing emails contained a link to a website controlled by i-Soon that was designed to mimic a sign-in website for the DIA (the "Fake DIA Website"), in the hope that DIA employees would enter their credentials into the Fake DIA Website. i-Soon then planned to use any DIA employee credentials

they obtained from the Fake DIA Website to impersonate DIA employees and access email inboxes and other files belonging to the DIA. i-Soon's attack was not successful.

Attack on Newspaper-2

25. Newspaper-2 is an American newspaper based in Manhattan.

26. In or around 2018, i-Soon, including CHEN CHENG, a/k/a "lengmo," a/k/a "Chief C," a/k/a "Jesse Chen," a/k/a "陈诚," WU HAIBO, a/k/a "shutd0wn," a/k/a "Boss Wu," a/k/a "吴海波," and WANG ZHE, a/k/a "ken73224," a/k/a "王哲," the defendants, and the MPS successfully compromised the contents of the corporate email account of an employee at Newspaper-2. To gain access to the account, the MPS used the tool sold by i-Soon that targeted Gmail accounts, described above in paragraph 12(e).

Attacks on the Department of Commerce and the International Trade Administration

27. The United States Department of Commerce ("DOC") is a Cabinet-level department within the United States government. The International Trade Administration ("ITA") is an agency within the DOC that promotes United States exports and defends against unfair trade practices.

28. In or around May 2018, LIANG GUODONG, a/k/a "梁国栋," the defendant, attempted to obtain access to the email inboxes of DOC and ITA employees by sending spear phishing emails to approximately sixty-three email accounts belonging to the DOC or the ITA. The spear phishing emails contained links to a website controlled by LIANG GUODONG, at the time a former i-Soon employee, that were designed to mimic sign-in websites for the DOC (the "Fake DOC Website") and the ITA (the "Fake ITA Website"), in the hope that DOC and ITA employees would enter their credentials into the Fake DOC Website and the Fake ITA Website. The DOC or ITA employee credentials obtained from the Fake DOC Website and the Fake ITA

Website could be used to impersonate DOC and ITA employees and to access email inboxes and other files belonging to the DOC and ITA. This attack was not successful, in part because ITA used multi-factor authentication.

Attack on Organization-1

29. Organization-1 is a religious organization based in the United States. Tens of thousands of churches and congregations are affiliated with Organization-1, and it has millions of members. Organization-1 has previously sent missionaries to China. The PRC government was interested in Organization-1's email accounts because it was a religious organization that has attempted to operate in China and was openly critical of the PRC government.

30. Prior to 2022, i-Soon employees compromised the email server of Organization-1.

31. Between in or about 2022 and 2023, i-Soon employees, including CHEN CHENG, a/k/a "lengmo," a/k/a "Chief C," a/k/a "Jesse Chen," a/k/a "陈诚," and WANG YAN, a/k/a "crysolo," a/k/a "王堰," the defendants, again compromised an email server belonging to Organization-1. i-Soon employees obtained access to approximately 200 email addresses of executives and employees of Organization-1.

32. Members of the conspiracy attempted to sell access to the email inboxes to the MSS and MPS, which resulted in further interest and direction from at least one such entity.

Attempted Attack on Organization-2

33. Organization-2 is a Texas-based organization focused on promoting human rights and religious freedom in China. Organization-2 was founded by a prominent critic of the PRC government.

34. In or around July 2018, an MPS officer directed i-Soon to compromise multiple email accounts belonging to Organization-2. The MPS officer identified a religious forum in

Chengdu featuring a pastor who had been associated with Organization-2 for years. The pastor had previously spoken out publicly about how the PRC government had suppressed his church.

35. In or around December 2019, i-Soon employees attempted to compromise the website of Organization-2.

36. In or around June 2020, an MPS officer directed i-Soon to compromise Organization-2.

Attack on News Service-1

37. News Service-1 is a news service funded by the United States government that delivers uncensored domestic news to audiences in Asian countries, including China. It is headquartered in Washington, D.C.

38. In approximately March 2019, i-Soon employees successfully compromised email accounts belonging to an online news service affiliated with News Service-1 and exfiltrated emails from those accounts.

39. In approximately June 2022, i-Soon employees again successfully compromised email accounts belonging to News Service-1 and exfiltrated emails from those accounts.

Attack on a Research University

40. University-1 is a state research university in the United States. From at least in or around February 2020 until at least April 2020, i-Soon employees successfully accessed computer systems at University-1, including at least approximately 21 user accounts at University-1. i-Soon employees then exfiltrated data from multiple systems at University-1. i-Soon also compromised a web server for a health sciences center at the university.

Attack on the New York State Assembly

41. The New York State Assembly (“NYSA”) is part of the legislature of the state of New York.

42. In or around July 2022, i-Soon employees attempted to access multiple email accounts belonging to NYSA, successfully compromised at least one such email account belonging to NYSA, and exfiltrated data from it.

43. i-Soon employees subsequently attempted to sell the emails stolen from NYSA to a number of MSS branch offices. i-Soon employees attempted to interest MSS officers in the stolen data with an email from members of a religious organization that is banned in China to a representative of NYSA.

i-Soon’s Attacks on Foreign Governments, Religious Leaders, and News Organizations

44. Between in or around 2017 and in or around 2022, i-Soon employees hacked or attempted to hack a series of victims outside of the United States. Most of the results of the computer intrusions were provided to the MSS or the MPS. i-Soon’s targets outside of the United States included news organizations, foreign governments, and a religious leader and personnel from his office.

Attack on Religious Leader-1 and His Office

45. Religious Leader-1 was a religious leader living outside China and the United States.

46. In or around 2017, i-Soon employees compromised several email accounts belonging to employees of Religious Leader-1 and attempted to sell access to those accounts to officers of the MSS and MPS.

47. In or around 2017, i-Soon employees obtained unauthorized access to the medical records for Religious Leader-1.

48. In or around 2018, i-Soon employees and the Shanghai MPS used i-Soon's Gmail tool, described in paragraph 12(e), to again compromise an email account belonging to an employee of Religious Leader-1.

Attack on Newspaper-3

49. Newspaper-3 is a newspaper based in Hong Kong that has actively covered the politics of Hong Kong and continues to do so today. Executive-1 has served as the Executive and Managing Director of Newspaper-3. i-Soon considered Newspaper-3 as being opposed to the PRC government and an important target.

50. In or around February 2017, at the direction of the MPS, i-Soon employees compromised the email account of Executive-1. i-Soon employees exfiltrated data from that email account and provided it to WANG LIYU, a/k/a "PICNIC350116," a/k/a "王立宇," the defendant, of the MPS.

51. In or around May 2017, i-Soon employees also provided data exfiltrated from the email account of Executive-1 to the MSS.

52. In or around October 2020, employees of i-Soon again attempted to access the servers of Newspaper-3.

Attacks on Foreign Jurisdictions

53. Members of the conspiracy attempted to sell the emails of foreign ministries to the MSS.

54. In or around June 2018, CHEN CHENG, a/k/a "lengmo," a/k/a "Chief C," a/k/a "Jesse Chen," a/k/a "陈诚," the defendant, an employee of i-Soon, sold the MSS unauthorized access to the contents of multiple email inboxes of employees of the foreign ministry of Taiwan. This access was obtained by a close associate of i-Soon. The MSS was particularly interested in

those email inboxes because they contained communications between Taiwanese officials and employees of the United States Department of State (the “State Department”).

55. In or around April 2022, CHEN CHENG, a/k/a “lengmo,” a/k/a “Chief C,” a/k/a “Jesse Chen,” a/k/a “陈诚,” the defendant, an employee of i-Soon, sold or attempted to sell the MPS unauthorized access to the contents of at least one email inbox of the foreign ministry of India, the Indian Ministry of External Affairs. This access was obtained by a close associate of i-Soon. The MPS was particularly interested in that email inbox because it contained communications between Indian officials and employees of the State Department. CHEN advertised that the email inbox contained information regarding a certain U.S. military capability. The close associate of i-Soon also stole emails from the Indian Ministry of External Affairs that were communications between the foreign ministries of India and Japan.

56. From at least in or around November 2022 until at least in or around December 2022, CHEN CHENG, a/k/a “lengmo,” a/k/a “Chief C,” a/k/a “Jesse Chen,” a/k/a “陈诚,” the defendant, a former employee of i-Soon, attempted to sell the MSS unauthorized access to the contents of multiple email inboxes of the foreign ministry of South Korea. The MSS was particularly interested in one of these email inboxes because that inbox was associated with one of South Korea’s offices in the United States. A close associate of i-Soon had previously obtained access to the email inboxes and had provided samples of their contents to CHEN. The close associate did not regain access to the email inboxes.

57. In or around 2022, CHEN CHENG, a/k/a “lengmo,” a/k/a “Chief C,” a/k/a “Jesse Chen,” a/k/a “陈诚,” the defendant, obtained unauthorized access to the contents of at least one email inbox of the foreign ministry of Indonesia. Those emails included internal memoranda of

Indonesia summarizing high-level and confidential diplomatic communications between Indonesia and the United States.

STATUTORY ALLEGATIONS

58. From at least in or around 2016 through in or around 2023, in the Southern District of New York and elsewhere, WU HAIBO, a/k/a “shutd0wn,” a/k/a “Boss Wu,” a/k/a “吴海波,” CHEN CHENG, a/k/a “lengmo,” a/k/a “Chief C,” a/k/a “Jesse Chen,” a/k/a “陈诚,” LIANG GUODONG, a/k/a “梁国栋,” MA LI, a/k/a “马丽,” WANG YAN, a/k/a “crysolo,” a/k/a “王堰,” WANG ZHE, a/k/a “ken73224,” a/k/a “王哲,” ZHOU WEIWEI, a/k/a “nullroot,” a/k/a “周伟伟,” XU LIANG, a/k/a “徐梁,” WANG LIYU, a/k/a “PICNIC350116,” a/k/a “王立宇,” SHENG JING, a/k/a “sjbible,” a/k/a “盛晶,” the defendants, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit offenses against the United States, to wit, computer intrusion, in violation of Title 18, United States Code, Sections 1030(a)(2)(C), 1030(a)(4), 1030(a)(5)(A), 1030(a)(6), 1030(c)(2)(A), 1030(c)(2)(B)(i) & (iii), 1030(c)(3)(A), and 1030(c)(4)(A)(i)(I), 1030(c)(4)(B)(i).

59. It was a part and an object of the conspiracy that WU HAIBO, a/k/a “shutd0wn,” a/k/a “Boss Wu,” a/k/a “吴海波,” CHEN CHENG, a/k/a “lengmo,” a/k/a “Chief C,” a/k/a “Jesse Chen,” a/k/a “陈诚,” LIANG GUODONG, a/k/a “梁国栋,” MA LI, a/k/a “马丽,” WANG YAN, a/k/a “crysolo,” a/k/a “王堰,” WANG ZHE, a/k/a “ken73224,” a/k/a “王哲,” ZHOU WEIWEI, a/k/a “nullroot,” a/k/a “周伟伟,” XU LIANG, a/k/a “徐梁,” WANG LIYU, a/k/a “PICNIC350116,” a/k/a “王立宇,” SHENG JING, a/k/a “sjbible,” a/k/a “盛晶,” the defendants, and others known and unknown, knowingly would and did cause the transmission of a program, information, code, and command, and as a result of such conduct, would and did intentionally cause damage, without authorization, to a protected computer, which would and did cause a loss (including loss resulting

from a related course of conduct affecting one and more other protected computers) aggregating to at least \$5,000 to one and more persons during any one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(A)(i)(I), and 1030(c)(4)(B)(i).

60. It was a further part and an object of the conspiracy that WU HAIBO, a/k/a “shutd0wn,” a/k/a “Boss Wu,” a/k/a “吴海波,” CHEN CHENG, a/k/a “lengmo,” a/k/a “Chief C,” a/k/a “Jesse Chen,” a/k/a “陈诚,” LIANG GUODONG, a/k/a “梁国栋,” MA LI, a/k/a “马丽,” WANG YAN, a/k/a “crysolo,” a/k/a “王堰,” WANG ZHE, a/k/a “ken73224,” a/k/a “王哲,” ZHOU WEIWEI, a/k/a “nullroot,” a/k/a “周伟伟,” XU LIANG, a/k/a “徐梁,” WANG LIYU, a/k/a “PICNIC350116,” a/k/a “王立宇,” SHENG JING, a/k/a “sjbible,” a/k/a “盛晶,” the defendants, and others known and unknown, knowingly and with the intent to defraud, would and did access a protected computer without authorization, and exceed authorized access, and by means of such conduct furthered the intended fraud and obtain something of value, that exceeded \$5,000 in a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(4) and 1030(c)(3)(A).

61. It was a further part and an object of the conspiracy that WU HAIBO, a/k/a “shutd0wn,” a/k/a “Boss Wu,” a/k/a “吴海波,” CHEN CHENG, a/k/a “lengmo,” a/k/a “Chief C,” a/k/a “Jesse Chen,” a/k/a “陈诚,” LIANG GUODONG, a/k/a “梁国栋,” MA LI, a/k/a “马丽,” WANG YAN, a/k/a “crysolo,” a/k/a “王堰,” WANG ZHE, a/k/a “ken73224,” a/k/a “王哲,” ZHOU WEIWEI, a/k/a “nullroot,” a/k/a “周伟伟,” XU LIANG, a/k/a “徐梁,” WANG LIYU, a/k/a “PICNIC350116,” a/k/a “王立宇,” SHENG JING, a/k/a “sjbible,” a/k/a “盛晶,” the defendants, and others known and unknown, would and did intentionally access computers without authorization, and exceed authorized access, and thereby would and did obtain information from a protected computer, for purposes of commercial advantage and private financial gain, and the value of the

information obtained would and did exceed \$5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B)(i) & (iii).

62. It was a further part and an object of the conspiracy that WU HAIBO, a/k/a “shutd0wn,” a/k/a “Boss Wu,” a/k/a “吴海波,” CHEN CHENG, a/k/a “lengmo,” a/k/a “Chief C,” a/k/a “Jesse Chen,” a/k/a “陈诚,” LIANG GUODONG, a/k/a “梁国栋,” MA LI, a/k/a “马丽,” WANG YAN, a/k/a “crysolo,” a/k/a “王堰,” WANG ZHE, a/k/a “ken73224,” a/k/a “王哲,” ZHOU WEIWEI, a/k/a “nullroot,” a/k/a “周伟伟,” XU LIANG, a/k/a “徐梁,” WANG LIYU, a/k/a “PICNIC350116,” a/k/a “王立宇,” SHENG JING, a/k/a “sjbible,” a/k/a “盛晶,” the defendants, and others known and unknown, knowingly and with the intent to defraud, would and did traffic in passwords and similar information through which computers may be accessed without authorization, in transactions affecting interstate and foreign commerce, and involving computers used by and for the Government of the United States, in violation of Title 18, United States Code, Sections 1030(a)(6) and 1030(c)(2)(A).

OVERT ACTS

63. In furtherance of the conspiracy and to effect the illegal objects thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. In or about December 2016, after WANG LIYU, a/k/a “PICNIC350116,” a/k/a “王立宇,” the defendant, directed that i-Soon attack News Service-1, XU LIANG, a/k/a “徐梁,” the defendant, carried out a DDoS attack on multiple websites controlled by News Service-1.

b. Between on or about May 5, 2017, and May 9, 2017, LIANG GUODONG, a/k/a “梁国栋,” the defendant, along with other i-Soon employees, including WANG YAN, a/k/a “crysolo,” a/k/a “王堰,” the defendant, exploited a vulnerability in the website of Newspaper-1,

headquartered in Manhattan, to compromise an email account belonging to Newspaper-1 and exfiltrate emails belong to the Chief Editor and a vice president of Newspaper-1.

c. In or about August 2017, MA LI, a/k/a “马丽,” and WANG YAN, a/k/a “crysolo,” a/k/a “王堰,” the defendants, participated in a cyberattack on accounts controlled by Individual-1 and his associates at the direction of the PRC Government.

d. In or about August 2017, ZHOU WEIWEI, a/k/a “nullroot,” a/k/a “周伟伟,” and CHEN CHENG, a/k/a “lengmo,” a/k/a “Chief C,” a/k/a “Jesse Chen,” a/k/a “陈诚,” the defendants, identified a list of organizations that have been critical of the Chinese Communist Party. i-Soon subsequently attacked one of the organizations on the list, News Service-1.

e. In or around September 2017, SHENG JING, a/k/a “sjbible,” a/k/a “盛晶,” the defendant, directed i-Soon to identify Internet Protocol addresses within China that had accessed the website of Newspaper-1 in order to assist the MPS in locating dissidents located in China.

f. In or around 2018, employees of i-Soon, including CHEN CHENG, a/k/a “lengmo,” a/k/a “Chief C,” a/k/a “Jesse Chen,” a/k/a “陈诚,” the defendant, provided the MPS with unauthorized access to the corporate email account of an employee at Newspaper-2, headquartered in Manhattan.

g. Domains used in connection with i-Soon’s hacking operations were registered in the name of WU HAIBO, a/k/a “shutd0wn,” a/k/a “Boss Wu,” a/k/a “吴海波,” the defendant, between in or about August 2013 and August 2019.

h. Between in or about October 2017 and in or about October 2018, a website used in i-Soon’s hacking operations was registered using an email address associated with LIANG

GUODONG, a/k/a “梁国栋,” the defendant, and an email address used to register spear phishing infrastructure was associated with LIANG.

i. Between 2016 and 2023, CHEN CHENG, a/k/a “lengmo,” a/k/a “Chief C,” a/k/a “Jesse Chen,” a/k/a “陈诚,” the defendant, sold information exfiltrated from email accounts hacked by i-Soon employees to the MPS and MSS for between the equivalent of \$10,000 and \$75,000 for each email inbox successfully hacked.

(Title 18, United States Code, Section 371.)

COUNT TWO
(Conspiracy to Commit Wire Fraud)

The Grand Jury further charges:

64. The allegations contained in paragraphs 1 through 64 of this Indictment are repeated and realleged as if fully set forth herein.

65. From in or around 2016 through in or around 2023, in the Southern District of New York and elsewhere, WU HAIBO, a/k/a “shutd0wn,” a/k/a “Boss Wu,” a/k/a “吴海波,” CHEN CHENG, a/k/a “lengmo,” a/k/a “Chief C,” a/k/a “Jesse Chen,” a/k/a “陈诚,” LIANG GUODONG, a/k/a “梁国栋,” MA LI, a/k/a “马丽,” WANG YAN, a/k/a “crysolo,” a/k/a “王堰,” WANG ZHE, a/k/a “ken73224,” a/k/a “王哲,” ZHOU WEIWEI, a/k/a “nullroot,” a/k/a “周伟伟,” XU LIANG, a/k/a “徐梁,” WANG LIYU, a/k/a “PICNIC350116,” a/k/a “王立宇,” SHENG JING, a/k/a “sjbible,” a/k/a “盛晶,” the defendants, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit wire fraud, in violation of Title 18, United States Code, Section 1343.

66. It was a part and an object of the conspiracy that WU HAIBO, a/k/a “shutd0wn,” a/k/a “Boss Wu,” a/k/a “吴海波,” CHEN CHENG, a/k/a “lengmo,” a/k/a “Chief C,” a/k/a “Jesse

Chen,” a/k/a “陈诚,” LIANG GUODONG, a/k/a “梁国栋,” MA LI, a/k/a “马丽,” WANG YAN, a/k/a “crysolo,” a/k/a “王堰,” WANG ZHE, a/k/a “ken73224,” a/k/a “王哲,” ZHOU WEIWEI, a/k/a “nullroot,” a/k/a “周伟伟,” XU LIANG, a/k/a “徐梁,” WANG LIYU, a/k/a “PICNIC350116,” a/k/a “王立宇,” SHENG JING, a/k/a “sjbible,” a/k/a “盛晶,” the defendants, and others known and unknown, knowingly having devised and intending to devise a scheme and artifice to defraud and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, to wit, the defendants and other members of the conspiracy used fraudulent means, including spear phishing, to obtain dominion and control over victim email accounts or computer networks with the intention of exfiltrating data from those victim accounts, which involved the use of interstate wires into and out of the Southern District of New York.

(Title 18, United States Code, Section 1349.)

FORFEITURE ALLEGATIONS

67. As a result of committing the offense alleged in Count One of this Indictment, WU HAIBO, a/k/a “shutd0wn,” a/k/a “Boss Wu,” a/k/a “吴海波,” CHEN CHENG, a/k/a “lengmo,” a/k/a “Chief C,” a/k/a “Jesse Chen,” a/k/a “陈诚,” LIANG GUODONG, a/k/a “梁国栋,” MA LI, a/k/a “马丽,” WANG YAN, a/k/a “crysolo,” a/k/a “王堰,” WANG ZHE, a/k/a “ken73224,” a/k/a “王哲,” ZHOU WEIWEI, a/k/a “nullroot,” a/k/a “周伟伟,” XU LIANG, a/k/a “徐梁,” WANG LIYU, a/k/a “PICNIC350116,” a/k/a “王立宇,” SHENG JING, a/k/a “sjbible,” a/k/a “盛晶,” the defendants, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 1030(i), any and all property, real or personal, constituting or derived from, any proceeds obtained

directly or indirectly, as a result of said offense, and any and all personal property that was used or intended to be used to commit or to facilitate the commission of said offense, including but not limited to a sum of money in United States currency representing the amount of proceeds traceable to the commission of said offense.

68. As a result of committing the wire fraud offense alleged in Count Two of this Indictment, WU HAIBO, a/k/a “shutd0wn,” a/k/a “Boss Wu,” a/k/a “吴海波,” CHEN CHENG, a/k/a “lengmo,” a/k/a “Chief C,” a/k/a “Jesse Chen,” a/k/a “陈诚,” LIANG GUODONG, a/k/a “梁国栋,” MA LI, a/k/a “马丽,” WANG YAN, a/k/a “crysolo,” a/k/a “王堰,” WANG ZHE, a/k/a “ken73224,” a/k/a “王哲,” ZHOU WEIWEI, a/k/a “nullroot,” a/k/a “周伟,” XU LIANG, a/k/a “徐梁,” WANG LIYU, a/k/a “PICNIC350116,” a/k/a “王立宇,” SHENG JING, a/k/a “sjbible,” a/k/a “盛晶,” the defendants, shall forfeit to the United States pursuant to Title 18, United States Code, Section 981(a)(1)(C), and Title 28, United States Code, Section 2461(c), any and all property, real and personal, that constitutes or is derived from proceeds traceable to the commission of said offense, including but not limited to a sum of money in United States currency representing the amount of proceeds traceable to the commission of said offense that the defendants personally obtained.

Substitute Assets Provision

69. If any 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 Title 21, United States Code, Section 853(p) and Title 28, United States Code, Section 2461(c), to seek forfeiture of any other property of the defendants up to the value of the above forfeitable property.

(Title 18, United States Code, Sections 981 and 1030;
Title 21, United States Code, Sections 853; and
Title 28, United States Code, Section 2461.)



FOREPERSON

Damian Williams

DAMIAN WILLIAMS
United States Attorney