IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Holding a Criminal Term
Grand Jury Sworn in on March 16, 2023

UNITED STATES OF AMERICA	:	**CRIMINAL NO.**
	:	
v.	:	**GRAND JURY ORIGINAL**
	:	
YIN KECHENG,	:	**VIOLATIONS:**
	:	
	:	**18 U.S.C. §§ 371, 1349, 1030, 1343, 1028A**
a/k/a "尹 可成,"	:	**(Conspiracy to Cause Damage To, and**
	:	**Obtain Information By Unauthorized**
ZHOU SHUAI,	:	**Access To, Protected Computers, to**
	:	**Commit Wire Fraud, and to Commit**
	:	**Aggravated Identity Theft)**
	:	
a/k/a "周帅"	:	**18 U.S.C. § 1343**
	:	**(Wire Fraud)**
Defendants.	:	
	:	**18 U.S.C. § 1030(a)(2)(C), (a)(4), (b),**
	:	**(c)(2)(B)**
	:	**(Obtaining Information By Unauthorized**
	:	**Access to Protected Computers)**
	:	
	:	**18 U.S.C. § 1030(a)(5)(A), (b), (c)(4)(B)**
	:	**(Intentionally Causing Damage to**
	:	**Protected Computers)**
	:	
	:	**18 U.S.C. § 1028A**
	:	**(Aggravated Identity Theft)**
	:	
	:	**18 U.S.C. § 1956(a)(2)(A)**
	:	**(Money Laundering)**
	:	
	:	**18 U.S.C. § 2**
	:	**(Aiding and Abetting)**
	:	
	:	**Criminal Forfeiture:**
	:	**18 U.S.C. § 981(a)(1)(C); 18 U.S.C.**
	:	**§ 982(a)(2); 18 U.S.C. § 1030(i) and (j);**
	:	**28 U.S.C. § 2461(c); and 21 U.S.C. §**
	:	**853(p).**

Case: 1:23-cr-00099
Assigned to: Judge Mehta, Amit P.
Assign Date: 3/28/2023
Description: INDICTMENT (B)
Related Case No: 18-cr-00126 (APM)

INDICTMENT

The Grand Jury charges that:

INTRODUCTION

At times material to this indictment:

1. Defendant YIN KECHENG ("YIN"), also known as "尹 可成" and "Ykcai," was a resident and citizen of the People's Republic of China ("PRC") who had no known residence or last known residence in the United States.

2. Defendant ZHOU SHUAI ("ZHOU"), also known as "周帅" and "Coldface," was a resident and citizen of the PRC who had no known residence or last known residence in the United States.

3. YIN and ZHOU have participated in a sophisticated computer hacking and data brokering scheme for a number of years. YIN and ZHOU have committed computer hacking (i.e., accessing protected computers without authorization and stealing data from compromised computers) and data brokering individually, in combination with one another, and in combination with others known and unknown to the Grand Jury, including with a former member of the PRC's People's Liberation Army.

4. Since at least June 2018 to and through November 2020, YIN and ZHOU have conspired with each other, and others known and unknown to the Grand Jury, including with a former member of the PRC's People's Liberation Army, to target and commit computer hacking offenses against technology companies, cleared defense contractors, governmental organizations, municipalities, and similar organizations in the United States and elsewhere, through the use of shared technology and computer infrastructure. YIN and ZHOU, together with the other conspirators, are collectively referred to here as the "conspirators."

5. The conspirators worked together to support each other's computer hacking and brokering of stolen data, including by sharing computer and internet infrastructure to target victim computer networks. To overcome network defenses and avoid detection, the conspirators employed a series of hacking tools, techniques and procedures over the course of the conspiracy. These tools and techniques included scanning target victim computer networks for vulnerabilities, pivoting from one area of the network to another to conduct reconnaissance once inside the victim network, and installing or utilizing malware that allowed the conspirators to communicate with other compromised networks, the conspirators' malicious servers, and other hacking infrastructure (including, as described below, command-and-control servers).

6. The conspirators obtained initial unauthorized access to protected computers using a variety of means, including by exploiting network vulnerabilities to gain unauthorized access or to perform unauthorized actions on the computer systems. The conspirators typically sought to convert their initial access into long-term, persistent access using several methods -- installing, on compromised computers, "web shells," which provided unauthorized access to victim networks, and virtual private network ("VPN") software.

7. The conspirators used command-and-control servers ("C2 servers") and "hop points" consisting of leased intermediary servers to control their malware and communicate with compromised protected computers. The intermediary or proxy servers were used by the conspirators to scan for network vulnerabilities, move within the network once they had gained unauthorized access, and exfiltrate data from victim computer networks for the conspirators' use and benefit. The conspirators also utilized techniques, such as deploying malicious code or malware, to maintain long-term access to the networks they compromised to allow for further exploitation or data exfiltration.

8. In or about 2019, the conspirators also exploited a publicly available security vulnerability. This technique allowed the conspirators to hack into protected computers using publicly available exploit code – without using their own distinctive or identifying malware – so long as the conspirators acted before victim companies updated their systems. This campaign included the use of the security vulnerability CVE-2019-0604. These compromises typically resulted in the installation of widely available web shells which were consistently used by the conspirators.

9. An underlying goal of the conspiracy was to obtain financial compensation by brokering stolen data from target victim computer networks. The conspirators, including YIN and ZHOU, worked together in furtherance of this goal by selling stolen data obtained in the course of computer hacking or by selling access to computer networks that they had compromised.

10. The conspirators executed the conspiracy using infrastructure of the type described in Paragraphs 5 and 7 in the United States, Europe, the PRC, and elsewhere in Asia and the world. The conspirators obtained that infrastructure for purposes of their computer hacking offenses, and they obtained it using, among other things, payments to providers inside the United States from outside of the United States originating from an account owned or controlled by a former member of the PRC's People's Liberation Army.

11. All of the conspirators known to the Grand Jury are foreign nationals, and none of the conspirators are known to have ever resided in the United States.

12. The targets of the conspirators included Victims A through G.

13. Victim A was a technology and defense industrial base company with over 400 employees that is headquartered in the United States. Victim A has contracted with customers

such as the Department of Defense, Department of Homeland Security, and government intelligence agencies. Victim A maintained computer servers in Virginia.

14. Victim B was a law firm headquartered in the United States with hundreds of attorneys across multiple offices. Victim B specialized in business and transactions, finance, intellectual property, litigation, and real estate law. Victim B maintained computer servers in Pennsylvania.

15. Victim C was a managed communications service provider company headquartered in the United States with over 500 employees. Victim C specialized in providing hosted Microsoft Exchange email, SharePoint, web conferencing, broadband, and Voice over Internet Protocol (VoIP) services. Victim C maintained computer servers in Georgia and Nevada.

16. Victim D was a government county municipality located in the United States with over 9,000 employees. Victim D maintained computer servers in Florida.

17. Victim E was an academic health system affiliated with a university located in the United States with a student body of over 3,000. Victim E included multiple hospitals and other facilities. Victim E maintained computer servers in California.

18. Victim F was a technology, engineering, and research organization headquartered in the United States. Victim F provided technical, integration, engineering, and analysis solutions to the U.S. government and other customers. Victim F maintained computer servers in Virginia.

19. Victim G was a think tank specializing in U.S. defense policy, force planning, and budgeting headquartered in the United States. Victim G maintained computer servers in the District of Columbia.

COUNT ONE

(Conspiracy to Cause Damage to and Obtain Unauthorized Access to Protected Computers, to Commit Wire Fraud, and to Commit Aggravated Identity Theft– Computer Hacking Conspiracy)

20. Paragraphs 1 through 19 are re-alleged here.

Overview of the Computer Hacking and Data Brokering Conspiracy

21. Beginning no later than June 2018 and continuing at least until November 2020, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, YIN KECHENG and ZHOU SHUAI, and other conspirators did knowingly and willfully combine, conspire, confederate, and agree with each other to commit the following offenses against the United States:

a. For the purposes of commercial advantage and private financial gain, and in furtherance of a criminal and tortious act in violation of the Constitution and the laws of the United States, that is, wire fraud, in violation of Title 18, United States Code, Section 1343, intentionally accessed, and attempted to access, computers without authorization, knowingly and with intent to defraud, and thereby obtained, and attempted to obtain, information from protected computers, the value of such information obtained exceeding $5,000, such conduct involving wires in interstate and foreign communication, in violation of Title 18, United States Code, Sections 1030(a)(2)(C), (a)(4) and (c)(2)(B)(i), (ii), and (iii);

b. Knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct, intentionally caused, or attempted to cause, damage without authorization to protected computers, and caused, or

attempted to cause, more than $5,000 loss in one year, and caused, or attempted to cause, damage affecting 10 or more protected computers during a 1-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B);

c. Devising, executing, and attempting to execute a scheme by means of false and fraudulent pretenses, representations, and promises, and caused the transmission of wire communications in interstate and foreign commerce various signals and sounds constituting wire transmissions for the purpose of executing such scheme or artifice to defraud, in violation of Title 18, United States Code, Section 1343; and

d. During and in relation to the crime of Wire Fraud, in violation of Title 18, United States Code, Section 1343, and the crime of Obtaining Information by Access to Protected Computers, in violation of Title 18, United States Code, Section 1030(a)(2)(C), did knowingly transfer, possess, and use without lawful authority, a means of identification of another person, in violation of Title 18, United States Code, Sections 1028A(a)(1), 1028A(b), 1028A(c)(4), (5), and 2.

in violation of Title 18, United States Code, Sections 371, 1030(a)(2), (a)(4), (c)(2)(B)(i), (ii), and (iii), 1030(a)(5)(A) and (c)(4)(B), 1343 and 1349, and 1028A.

Object of the Conspiracy

22. The object of the conspiracy was for the defendants to commit computer intrusions and gain and maintain unauthorized access to victims' computers to accomplish the following objectives, among others, depending on the particular intrusion: (i) create and maintain illegal, unauthorized access to victims' networks; (ii) steal victims' data; and, (iii) profit by brokering or

selling victim data, or profit by brokering or selling the ability to surreptitiously access victims' computers and networks.

Manner and Means of the Conspiracy

23. As part of the conspiracy, the conspirators supported one another, and aided and abetted computer hacking committed by one another, by sharing computer hacking infrastructure, including C2 servers and hop point servers, as well as malware and information about malware, and tactics, techniques, and procedures for successfully committing computer intrusions targeting protected computers.

24. As part of the conspiracy, the conspirators used a variety of malicious techniques, including deploying and using malware, in order to gain and maintain unauthorized access to protected computers that were connected to the Internet.

25. As part of the conspiracy, the conspirators obtained the use of Internet-connected computer servers, typically by leasing remote access to them, directly or indirectly from web hosting providers. These computer servers were used to register and access operational e-mail accounts, to send commands to (and receive valuable information from) victim computers, and to fraudulently obtain access to protected computers and information stored on those computers. These computer servers also served as hop points between the computers owned by members of the conspiracy and victim computers, and were used to obfuscate the conspirators' identities.

26. As part of the conspiracy, the conspirators utilized leased servers to scan victim computers for vulnerabilities and to exploit such vulnerabilities to gain and maintain unauthorized access to the victim computers and networks. Through this unauthorized access, the conspirators installed and accessed malware that allowed the conspirators to identify, collect, and exfiltrate information stored on the victim computers.

27. As part of the conspiracy, the conspirators used stolen network credentials to gain access to victim computers and networks to steal data.

28. As part of the conspiracy, the conspirators used multiple foreign-based and United States-based e-mail, social media, and other online accounts to interface with each other, with other conspirators for particular schemes, and with internet service providers, web hosting providers, and victim computers.

29. As part of the conspiracy, the conspirators communicated with customers who wished to purchase information or access to information obtained from victim computers through unauthorized means.

30. Following their unauthorized internal access to victim networks, as part of the conspiracy, the conspirators made efforts to mask their presence in order to maintain persistent and long-term access. As a result of their unlawful intrusions and access, the conspirators caused damage to victim networks that exceeded millions of dollars in remediation costs. As part of their long-term access, the conspirators stole data from the victim networks that was later brokered to other individuals.

31. For example, as part of the conspiracy, the conspirators stole internal organizational work product from a think tank and multinational conglomerate company that related to Russia, the PRC, electro-magnetic weapons, and Warship Design Centers. The conspirators then sold the data and/or access to such data interested customers.

32. The conspirators, to include YIN, conducted their intrusions for the purpose of raising money to purchase personal items.

33. The conspirators, to include ZHOU, discussed pricing the stolen data and/or access to the stolen data to be resold to interested clients.

34. The conspirators, to include ZHOU, discussed specific material obtained through computer intrusions, including material ZHOU believed was related to an American-made attack helicopter.

35. The conspirators, to include ZHOU, discussed enlisting other hacking groups so that the conspirators could offer clients the ability to conduct, for a fee, a large-scale network attack.

OVERT ACTS

36. In furtherance of the conspiracy, the following overt acts were committed beginning outside of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia:

a. Beginning on or about June 28, 2018, and continuing until at least July 8, 2020, multiple servers were leased from a foreign-based company. These servers were used by the conspirators as C2 servers and hop points to scan and connect with victim computers, and to exfiltrate information from victim computers.

b. Beginning on or about June 3, 2019, and continuing until at least August 1, 2019, multiple additional servers were leased from a second foreign-based company. These servers were used by the conspirators as C2 servers and hop points to scan and connect with victim computers and to exfiltrate information from victim computers.

c. On June 3, 2019, the conspirators transferred a .002472 bitcoin payment to a foreign-based virtual private server ("VPS") provider, which was wired through a U.S. correspondent bitcoin payment processor.

d. On June 17, 2019, the conspirators transferred a .002185 bitcoin payment to a foreign-based VPS provider, which was wired through a U.S. correspondent bitcoin payment processor.

e. Beginning on or about June 17, 2019, and continuing until at least June 27, 2019, a hop point used by YIN made multiple exfiltration requests to an unauthorized web shell installed on the network of Victim A.

f. On June 24, 2019, the conspirators transferred a .001946 bitcoin payment to a foreign-based VPS provider, which wired through a U.S. correspondent bitcoin payment processor.

g. On June 24, 2019, the conspirators transferred a .001932 bitcoin payment to a foreign-based VPS provider, which wired through a U.S. correspondent bitcoin payment processor.

h. On June 25, 2019, the conspirators transferred a .016878 bitcoin payment to a foreign-based VPS provider, which wired through a U.S. correspondent bitcoin payment processor.

i. On June 26, 2019, and June 27, 2019, a hop point used by YIN made connections to an unauthorized web shell installed on the network of Victim A.

j. On June 27, 2019, an IP address associated with one of YIN's personal accounts made an exfiltration request to an unauthorized web shell installed on the network of Victim A.

k. On June 29, 2019, the conspirators transferred a .001795 bitcoin payment to a foreign-based VPS provider, which wired through a U.S. correspondent bitcoin payment processor.

l. On July 1, 2019, a hop point used by YIN made connections to two different web shells installed on the network of Victim B.

m. Beginning on or about July 4, 2019, and continuing until at least November 17, 2020, ZHOU brokered data and/or access to data gained through the intrusions into Victim G's network conducted by the conspirators for commercial advantage and financial gain.

n. Beginning on or about July 4, 2019, and continuing until at least November 17, 2020, ZHOU brokered data and/or access to data gained through intrusions into a foreign nation's Ministry of Foreign Affairs' network conducted by the conspirators for commercial advantage and financial gain.

o. On July 8, 2019, the conspirators transferred a .001721 bitcoin payment to a foreign-based VPS provider, which wired through a U.S. correspondent bitcoin payment processor.

p. On July 15, 2019, the conspirators transferred a .001923 bitcoin payment to a foreign-based VPS provider, which wired through a U.S. correspondent bitcoin payment processor.

q. On July 29, 2019, the conspirators transferred a .002021 bitcoin payment to a foreign-based VPS provider, which wired through a U.S. correspondent bitcoin payment processor.

r. On July 29, 2019, the conspirators transferred a .00202 bitcoin payment to a foreign-based VPS provider, which wired through a U.S. correspondent bitcoin payment processor.

s. On August 12, 2019, the conspirators transferred a .001762 bitcoin payment to a foreign-based VPS provider, which wired through a U.S. correspondent bitcoin payment processor.

t. On August 29, 2019, a hop point used by YIN accessed a web shell installed on the network of Victim D on July 13, 2019. Beginning on July 29, 2019, and continuing until at least September 11, 2019, an account used by YIN accessed the initial hop point used on August 29, 2019 to access the web shell on Victim D's network.

u. On September 2, 2019, the conspirators transferred a .001959 bitcoin payment to a foreign-based VPS provider, which wired through a U.S. correspondent bitcoin payment processor.

v. On September 2, 2019, the conspirators transferred a .001958 bitcoin payment to a foreign-based VPS provider, which wired through a U.S. correspondent bitcoin payment processor.

w. On October 8, 2019, the conspirators transferred a .002316 bitcoin payment to a foreign-based VPS provider, which wired through a U.S. correspondent bitcoin payment processor.

x. On October 12, 2019, the conspirators transferred a .002304 bitcoin payment to a foreign-based VPS provider, which wired through a U.S. correspondent bitcoin payment processor.

y. On December 3, 2019, a hop point used by the conspirators made an exfiltration request for a file of archived data of employee email accounts controlled by Victim B.

z. On February 15, 2020, a hop point used by YIN scanned Victim C's network for potential vulnerabilities. On March 18, 2020, the same hop point used by YIN made an exfiltration request to an unauthorized web shell installed on the network of Victim C.

aa. Beginning on or about January 16, 2020, and continuing until at least November 17, 2020, ZHOU brokered data and/or access to data gained through the intrusions into Victim A's network conducted by the conspirators for commercial advantage and financial gain.

bb. Beginning on or about January 16, 2020, and continuing until at least November 17, 2020, ZHOU brokered data and/or access to data gained through intrusions into a foreign-based multinational conglomerate company's network conducted by the conspirators for commercial advantage and financial gain.

cc. Beginning on or about January 16, 2020, and continuing until at least November 17, 2020, YIN used hop points to exfiltrate data from the network of a foreign-based multinational conglomerate company through an exploited network vulnerability, to a server associated with one of YIN's personal accounts. Analysis of the server revealed scans for data in directories with names such as "electro-magnetic weapons" and "Warship Design Centers."

dd. Beginning on or about January 16, 2020, and continuing until at least November 17, 2020, ZHOU brokered data and/or access to data gained through intrusions into a foreign political and economic union organization's network conducted by the conspirators for commercial advantage and financial gain.

ee. Beginning on or about January 16, 2020, and continuing until at least November 17, 2020, ZHOU brokered data and/or access to data gained through intrusions into a foreign nation's Ministry of Finance's network conducted by the conspirators for commercial advantage and financial gain.

ff. Beginning on or about January 16, 2020, and continuing until at least November 17, 2020, ZHOU brokered data and/or access to data gained through intrusions into a foreign nation's Ministry of Foreign Affairs' network conducted by the conspirators for commercial advantage and financial gain.

gg. Beginning on or about January 16, 2020, and continuing until at least November 17, 2020, ZHOU brokered data and/or access to data gained through intrusions into a foreign nation's Ministry of Foreign Affairs' network conducted by the conspirators for commercial advantage and financial gain.

hh. Between February 14, 2020, and March 1, 2020, a hop point used by YIN scanned Victim E's network for potential vulnerabilities.

ii. Beginning on or about February 14, 2020, and continuing until at least March 4, 2020, the conspirators used hop points to exfiltrate data from Victim G's network through an exploited network vulnerability, to a server associated with one of YIN's personal accounts. Analysis of the server revealed such data included identifiers such as "Russia" and "China."

jj. Beginning on or about March 2, 2020, and continuing until at least March 4, 2020, a hop point used by YIN accessed multiple unauthorized web shells installed on the network of Victim E.

kk. On March 3, 2020, the conspirators used stolen user credentials of a customer of Victim C to gain unauthorized access to Victim C's network.

ll. On April 6, 2020, the conspirators used stolen user credentials of customers of Victim C to gain unauthorized access to Victim C's network.

mm. On April 17, 2020, April 27, 2020, and May 15, 2020, the conspirators used hop point servers to gain unauthorized access to the network of Victim F. Beginning on or about May 13, 2020, and continuing until at least May 17, 2020, an IP address associated with one of YIN's personal accounts made exfiltration requests to one of the hop point servers used by the conspirators to access the network of Victim F.

nn. On April 17, 2020, the conspirators gained unauthorized access to the Microsoft Exchange mailbox of Victim F employee S.A. by utilizing password information previously obtained in the intrusion of the network of Victim F.

oo. On April 27, 2020, the conspirators gained unauthorized access to the Microsoft Exchange mailbox of Victim F employee M.R. by utilizing password information previously obtained in the intrusion of the network of Victim F.

pp. On May 15, 2020, the conspirators gained unauthorized access to the Microsoft Exchange mailbox of Victim F employee R.E. of by utilizing password information previously obtained in the intrusion of the network of Victim F.

(**Conspiracy**, in violation of Title 18, United States Code, Sections 371, 1030(a)(2)(C) and (c)(2)(B)(i) and (ii), 1030(a)(5)(A) and (c)(4)(B)(i)), 1349 and 1343, and 1028A.

COUNT TWO
(Wire Fraud - Victim A)

37. Paragraphs 1 through 19 and 22 through 36 are re-alleged here.

38. Beginning on or about June 17, 2019, and continuing until at least June 27, 2019, beginning outside the jurisdiction of any particular State or district, and pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, YIN and ZHOU, for the purpose of executing the scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and by concealment of material facts, and attempting to do so, did transmit, direct, and cause to be transmitted, by means of wire communications in interstate and foreign commerce between the PRC and the Commonwealth of Virginia, writings, signs, and signals, namely electronic connections between a hop point and a computer belonging to Victim A, for the purpose of obtaining proprietary and valuable information from Victim A.

(**Wire Fraud**, in violation of Title 18, United States Code, Sections 1343 and 2).

COUNT THREE
(Wire Fraud – Victim B)

39. Paragraphs 1 through 19 and 22 through 36 are re-alleged here.

40. On or about June 10, 2019 and continuing until at least January 6, 2020, beginning outside the jurisdiction of any particular State or district, and pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, YIN and ZHOU, for the purpose of executing the scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and by concealment of material facts, and attempting to do so, did transmit and cause to be transmitted, by means of wire communications in interstate and foreign commerce between the PRC and the State of Pennsylvania, writings, signs, and signals which comprised communications exchanging electronic information between hop points and computers belonging to Victim B, for the purpose of obtaining proprietary and valuable information from Victim B.

(**Wire Fraud**, in violation of Title 18, United States Code, Sections 1343 and 2).

COUNT FOUR
(Wire Fraud – Victim C)

41. Paragraphs 1 through 19 and 22 through 36 are re-alleged here.

42. On or about February 15, 2020, and continuing until at least April 6, 2020, beginning outside the jurisdiction of any particular State or district, and pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, YIN and ZHOU, for the purpose of executing the scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and by concealment of material facts, and attempting to do so, did transmit and cause to be transmitted, by means of wire communications in interstate and foreign commerce between the PRC and the Commonwealth of Virginia, writings, signs, and signals which comprised communications exchanging electronic information between hop points and computers belonging to Victim C, for the purpose of obtaining proprietary and valuable information from Victim C.

(**Wire Fraud**, in violation of Title 18, United States Code, Sections 1343 and 2).

COUNT FIVE
(Wire Fraud – Victim D)

43. Paragraphs 1 through 19 and 22 through 36 are re-alleged here.

44. On or about June 16, 2019, and continuing until at least August 29, 2019, beginning outside the jurisdiction of any particular State or district, and pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, YIN and ZHOU, for the purpose of executing the scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and by concealment of material facts, and attempting to do so, did transmit and cause to be

transmitted, by means of wire communications in interstate and foreign commerce between the PRC, and the State of Florida, writings, signs, and signals which comprised communications exchanging electronic information between a hop point and computers belonging to Victim D, for the purpose of obtaining proprietary and valuable information from Victim D.

(**Wire Fraud**, in violation of Title 18, United States Code, Sections 1343 and 2).

COUNT SIX
(Wire Fraud – Victim E)

45. Paragraphs 1 through 19 and 22 through 36 are re-alleged here.

46. On or about February 14, 2020, and continuing until at least April 26, 2020, beginning outside the jurisdiction of any particular State or district, and pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, YIN and ZHOU, for the purpose of executing the scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and by concealment of material facts, and attempting to do so, did transmit and cause to be transmitted, by means of wire communications in interstate and foreign commerce between the PRC and the State of California, writings, signs, and signals which comprised communications exchanging electronic information between a hop point and computers belonging to Victim E, for the purpose of obtaining proprietary and valuable information from Victim E.

(**Wire Fraud**, in violation of Title 18, United States Code, Sections 1343 and 2).

COUNT SEVEN
(Wire Fraud – Victim F)

47. Paragraphs 1 through 19 and 22 through 36 are re-alleged here.

48. Between on or about April 13, 2020, and continuing until at least May 18, 2020, beginning outside the jurisdiction of any particular State or district, and pursuant to Title 18, United

States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, YIN and ZHOU, for the purpose of executing the scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and by concealment of material facts, and attempting to do so, did transmit and cause to be transmitted, by means of wire communications in interstate and foreign commerce between the PRC, and the Commonwealth of Virginia, writings, signs, and signals which comprised communications exchanging electronic information between a hop point and computers belonging to Victim F, for the purpose of obtaining proprietary and valuable information from Victim F.

(**Wire Fraud**, in violation of Title 18, United States Code, Sections 1343 and 2).

COUNT EIGHT
(Wire Fraud – Victim G)

49. Paragraphs 1 through 19 and 22 through 36 are re-alleged here.

50. Between on or about February 14, 2020, and March 18, 2020, beginning outside the jurisdiction of any particular State or district, and pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, YIN and ZHOU, for the purpose of executing the scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and by concealment of material facts, and attempting to do so, did transmit and cause to be transmitted, by means of wire communications in interstate and foreign commerce between the PRC, and the District of Columbia, writings, signs, and signals which comprised communications exchanging electronic information between hop points and computers belonging to Victim G, for the purpose of obtaining proprietary and valuable information from Victim G.

(**Wire Fraud**, in violation of Title 18, United States Code, Sections 1343 and 2).

COUNT NINE - FIFTEEN

(Obtaining Information by Unauthorized Access to Protected Computers)

51. Paragraphs 1 through 19 and 22 through 36 are re-alleged here.

52. On or about the dates listed below, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, and for purposes of commercial advantage and private financial gain, and in furtherance of a criminal and tortious act in violation of the Constitution and the laws of the United States, that is, wire fraud, in violation of Title 18, United States Code, Section 1343, YIN and ZHOU directed to intentionally access, caused to intentionally access, attempted to intentionally access, and did intentionally access a protected computer without authorization, and thereby obtained information from a protected computer belonging to the below victims which had value in excess of $5,000.

COUNT	VICTIM	DATE
Nine	A	On or about June 17, 2019, and continuing until at least June 27, 2019
Ten	B	On or about June 10, 2019 and continuing until at least January 6, 2020
Eleven	C	On or about February 15, 2020, and continuing until at least April 6, 2020
Twelve	D	On or about June 16, 2019, and continuing until at least August 29, 2019
Thirteen	E	On or about February 14, 2020, and continuing until at least April 26, 2020
Fourteen	F	On or about April 13, 2020, and continuing until at least May 18, 2020

Fifteen	G	On or about February 14, 2020, and continuing until at least March 18, 2020

(**Obtaining Information by Unauthorized Access to a Protected Computer**, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(B)(i), (ii), (iii) and 2)

COUNT SIXTEEN - TWENTY-TWO
(Intentional Damage to a Protected Computer)

53. Paragraphs 1 through 19 and 22 through 36 are re-alleged here.

54. On or about the dates listed below, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, YIN and ZHOU, knowingly attempted to cause, and did cause, the transmission of a program, information, code, and command, and, through such conduct, intentionally caused damage without authorization to protected computers belonging to the victims below, and thereby would and did intentionally cause loss to one or more persons during a one-year period from the defendants' course of conduct affecting protected computers aggregating at least $5,000 in value, and which damage affected 10 or more protected computers during a one-year period.

COUNT	VICTIM	DATE
Sixteen	A	On or about June 17, 2019, and continuing until at least June 27, 2019
Seventeen	B	On or about June 10, 2019 and continuing until at least January 6, 2020
Eighteen	C	On or about February 15, 2020, and continuing until at least April 6, 2020

Nineteen	D	On or about June 16, 2019, and continuing until at least August 29, 2019
Twenty	E	On or about February 14, 2020, and continuing until at least April 26, 2020
Twenty-One	F	On or about April 13, 2020, and continuing until at least May 18, 2020
Twenty-Two	G	On or about February 14, 2020, and continuing until at least March 18, 2020

(**Intentional Damage to a Protected Computer**, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B) and 2)

COUNT TWENTY-THREE
(Aggravated Identity Theft – Employees of Victim C)

55. Paragraphs 1 through 19 and 22 through 36 are re-alleged here.

56. On March 3, 2020, and April 6, 2020, during and in relation to the crime of Wire Fraud, in violation of Title 18, United States Code, Section 1343, and the crime of Obtaining Information by Access to Protected Computers, in violation of Title 18, United States Code, Section 1030(a)(2)(C), YIN, ZHOU, and other conspirators did knowingly transfer, possess, and use without lawful authority, a means of identification of another person, namely, O., C.S., and M.A., customers of Victim C.

(**Aggravated Identity Theft,** in violation of Title 18, United States Code, Sections 1028A(a)(1), 1028A(b), 1028A(c)(4), (5), and 2)

COUNT TWENTY-FOUR
(Aggravated Identity Theft – Employees of Victim F)

57. Paragraphs 1 through 19 and 22 through 36 are re-alleged here.

58. On April 17, 2020, April 27, 2020, and May 15, 2020, during and in relation to the crime of Wire Fraud, in violation of Title 18, United States Code, Section 1343, and the crime of Obtaining Information by Access to Protected Computers, in violation of Title 18, United States

Code, Section 1030(a)(2)(C), YIN, ZHOU, and other conspirators did knowingly transfer, possess, and use without lawful authority, a means of identification of another person, namely, S.A., T.T., K.F., M.M., M.G., D.S., M.R., R.E., L.D., T.F., employees of Victim F.

(**Aggravated Identity Theft,** in violation of Title 18, United States Code, Sections 1028A(a)(1), 1028A(b), 1028A(c)(4), (5), and 2)

COUNT TWENTY-FIVE
(Money Laundering)

59. Paragraphs 1 through 19 and 22 through 36 are re-alleged here.

60. On June 3, 2019, June 17, 2019, June 24, 2019, June 25, 2019, June 29, 2019, July 8, 2019, July 15, 2019, July 29, 2019, August 12, 2019, September 2, 2019, October 8, 2019, and October 12, 2019, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, YIN, ZHOU, and other conspirators knowingly transported, transmitted, and transferred funds, and aided, abetted and willfully caused, the transport, transmitting, and transfer of funds, that is, bitcoin payments in total valued at approximately $466.35 for the lease of servers, to a place in the United States from and through a place outside the United States, with the intent to promote the carrying on of specified unlawful activity, that is, intentionally damaging, and obtaining information by unauthorized access to, protected computers, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(a)(2)(C), and wire fraud, in violation of Title 18, United States Code, Section 1343.

(**Money Laundering,** in violation of Title 18, United States Code, Sections 1956(a)(2)(A) and 2)

FORFEITURE ALLEGATION

1. Upon conviction of any offenses alleged in Counts 1, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, and/or 22 of this Indictment, the defendants shall forfeit to the United States any

property constituting, or derived from, proceeds that the defendants obtained directly or indirectly, as the result of these violations, pursuant to 18 U.S.C. § 982(a)(2)(B). The United States will also seek a forfeiture money judgment against the defendants equal to the value of any property constituting, or derived from, proceeds that the defendants obtained directly or indirectly, as the result of these violations.

2. Upon conviction of any of the offenses alleged in Counts 1, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, and/or 22 of this Indictment, the defendants shall forfeit to the United States: (a) the defendant's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of these violations; (b) any property, real or personal, constituting or derived from, any proceeds the defendants obtained, directly or indirectly, as a result of these violations; (c) any person property used or intended to be used to commit or to facilitate the commission of these violations; and (d) any property, real or personal, which constitutes or is derived from proceeds traceable to these violations, pursuant to 18 U.S.C. §§ 1030(i) and (j). The United States will also seek a forfeiture money judgment against the defendants equal to the value of this property.

3. Upon conviction of any of the offenses alleged in Counts 1, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, and/or 22 of this Indictment, the defendant shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds traceable to these offenses, pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c). The United States will also seek a forfeiture money judgment against the defendant equal to the value of any property, real or personal, which constitutes or is derived from proceeds traceable to these offenses.

4. Upon conviction of the offense alleged in Count 25 of this Indictment, the defendants shall forfeit to the United States any property, real or personal, involved in this offense or any property traceable to such property, pursuant to 18 U.S.C. § 982(a)(1). The United States will also seek a forfeiture money judgment against the defendants equal to the value of any property, real or personal, involved in this offense, or any property traceable to such property.

5. If any of the property described above as being subject to forfeiture, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the Court;

d. has been substantially diminished in value; or

e. has been commingled with other property that cannot be divided without difficulty;

the defendant shall forfeit to the United States any other property of the defendant, up to the value of the property described above, pursuant to 21 U.S.C. § 853(p).

(**Criminal Forfeiture,** pursuant to Title 18, United States Code, Section 981(a)(1)(C), Title 28, United Sates Code, Section 2461(c), Title 18, United States Code, Sections 982(a)(1) and 982(a)(2), Title 18, United States Code, Sections 1030(i) and (j), and Title 21, United States Code, Section 853(p)).

A TRUE BILL

_____

Foreperson

MATTHEW M. GRAVES
UNITE STATES ATTORNEY