

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Holding a Criminal Term
Grand Jury Sworn in on May 7, 2019

UNITED STATES OF AMERICA	:	CRIMINAL NO.
	:	
v.	:	GRAND JURY ORIGINAL
	:	
ZHANG HAORAN,	:	VIOLATIONS:
	:	18 U.S.C. §§ 371, 1030
a/k/a “张浩然,”	:	(Conspiracy To Cause Damage To, and
	:	Obtain Information By Unauthorized
TAN DAILIN,	:	Access To, Protected Computers)
	:	
a/k/a “谭戴林,”	:	18 U.S.C. §§ 1349, 1343
	:	(Conspiracy To Commit Wire Fraud)
Defendants.	:	
	:	18 U.S.C. § 1343
	:	(Wire Fraud)
	:	
	:	18 U.S.C. §§ 1030(a)(2), (c)(2)(B)
	:	(Obtaining Information By Unauthorized
	:	Access To Protected Computers)
	:	
	:	18 U.S.C. §§ 1030(a)(5A), (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).

INDICTMENT

Case: 19-cr-274
Assigned To: Judge Amit P. Mehta
Assign. Date: 8/15/2019
Description: INDICTMENT (B)

The Grand Jury charges that:

INTRODUCTION

At times material to this indictment:

1. Defendant Zhang HaoRan (“ZHANG”), also known as “张浩然,” was a resident of the People’s Republic of China (“PRC”). ZHANG had no known residence or past residence within the United States. ZHANG was a sophisticated and advanced computer hacker.

2. Defendant Tan DaiLin (“TAN”), also known as “谭戴林,” was a resident of the PRC. TAN had no known residence or past residence within the United States. TAN was a sophisticated and advanced computer hacker.

3. ZHANG and TAN have been participating in sophisticated computer hacking for years. ZHANG and TAN have committed computer hacking individually, in combination with one another, and in combination with others known and unknown to the Grand Jury.

4. Since at least May 2011, ZHANG and TAN have conspired with each other, and with others known and unknown to the Grand Jury, to commit computer hacking offenses targeting high-technology and similar organizations in the United States and elsewhere, through the use of shared computer hacking technology and computer infrastructure. ZHANG and TAN, together with the other conspirators who have conspired to target high-technology and similar organizations through shared technology and infrastructure, are collectively referred to here as the “Computer Hacking Conspirators.”

5. The Computer Hacking Conspirators worked together to support each other’s computer hacking, including by sharing computer and internet infrastructure that has been used to target victim computer networks. Their group employed similar hacking tools and techniques over

the course of the conspiracy, which evolved over time, demonstrating advances in tradecraft and overcoming network defenses. This tradecraft included traditional spear-phishing e-mails, with attached malware that communicated with the Computer Hacking Conspirators' malicious domains, servers, and other hacking infrastructure (including, as described below, command and control "dead drops"). The tradecraft also included more sophisticated methods, including "supply chain attacks" that not only victimized software development companies, but also provided the conspirators with a foothold to victimize the companies' third-party customers.

6. All of the Computer Hacking Conspirators are foreign nationals, and none of the Computer Hacking Conspirators are known to have ever resided in the United States.

7. As another way to make money, and since at least November 2014, ZHANG and TAN have participated in an additional conspiracy, together with others known and unknown to the Grand Jury, to target organizations and individuals associated with the video game industry. ZHANG and TAN, together with the other participants in this conspiracy, are collectively referred to here as the "Video Game Conspirators."

8. Specifically, since at least November 2014, ZHANG and TAN, conspiring with other Video Game Conspirators, have obtained unauthorized access to video game company computer networks for the purpose of accessing the companies' databases and fraudulently obtaining and otherwise generating digital items of value, including video game currency and other digital items directly related to video games. These digital items (*e.g.*, points, powers, or other digital goods referred to collectively as "gaming artifacts") could be used to extend or enhance the game-playing experience for video game players. However, Video Game Conspirators did not

illegally obtain gaming artifacts merely for their own entertainment. Rather, they illegally obtained and generated gaming artifacts for the specific purpose of selling them for a profit.

9. ZHANG, TAN, and the other Video Game Conspirators used many of the same sophisticated and evolving techniques, malware, and computer infrastructure used by the Computer Hacking Conspirators. Additionally, using their unauthorized access to corporate networks, the Video Game Conspirators also monitored the video game companies' fraud detection teams that were working to identify and counter the conspiracy's scheme, which allowed them to evade detection. The Video Game Conspirators also used their unauthorized computer access to take action against other unrelated groups engaged in the same fraudulent generation of gaming artifacts, thereby attempting to eliminate the criminal competition.

10. All of the Video Game Conspirators are foreign nationals, and none of the Video Game Conspirators are known to have ever resided in the United States.

11. The targets of the Video Game Conspirators included VICTIMS A through F.

12. VICTIM A was a company associated with the video game industry. VICTIM A maintained computer servers in New York.

13. VICTIM B was a company associated with the video game industry. VICTIM B maintained computer servers in Texas.

14. VICTIM C was an individual who worked for a software company. VICTIM C resided in the United Kingdom.

15. VICTIM D was a company associated with the video game industry. VICTIM D maintained computer servers in the State of Washington.

16. VICTIM E was a company associated with the video game industry. VICTIM E maintained computer servers in Illinois.

17. VICTIM F was a company associated with the video game industry. VICTIM F maintained computer servers in California.

COUNT ONE
(Conspiracy to Cause Damage To and Obtain Unauthorized Access To Protected Computers – Computer Hacking Conspiracy)

18. Paragraphs 1 through 17 are re-alleged here.

Overview of the Computer Hacking Conspiracy

19. Beginning no later than about May 2011 and continuing at least until November 2018, 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, ZHANG HAORAN, TAN DAILIN, and other Computer Hacking Conspirators did knowingly and willfully combine, conspire, confederate, and agree with each other to commit the following offenses against the United States:

- a. 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, intentionally accessed, and attempted to access, computers without authorization, and thereby obtained, and attempted to obtain, information from protected computers, such conduct involving wires in interstate and foreign communication, in violation of Title 18, United States Code, Sections 1030(a)(2) and (c)(2)(B)(i) and (ii); and

- 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 in 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);

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

Objects, Manners, and Means of the Computer Hacking Conspiracy

20. The objects of the Computer Hacking Conspiracy were to commit computer intrusions and wire fraud, in the United States and elsewhere, and to install malware on protected computers, to damage such computers, to gain unauthorized access to those and other protected computers, to obtain information of value that belonged to the owners and users of the targeted protected computers, and to do so by means materially false and fraudulent representations and pretenses, and to thereby fraudulently obtain money, property, and other things of value, including from the owners of protected computers.

21. As part of the conspiracy, the Computer Hacking Conspirators supported one another, and aided and abetted computer hacking committed by one another, by sharing computer hacking infrastructure, including command and control (or “C2”) servers, as well as malware and information about malware, and tactics, techniques, and procedures for successfully committing computer intrusions targeting protected computers.

22. As part of the conspiracy, the Computer Hacking Conspirators used multiple and evolving sets of sophisticated malware to gain and maintain unauthorized access to protected computers that were connected to the Internet.

23. As part of the conspiracy, the Computer Hacking Conspirators, in some instances, sent fraudulent “spear-phishing” e-mails, that is, e-mails which appeared to be legitimate messages with innocent attachments (such as purported résumés), but which in fact contained fraudulent attachments or links which would install malware on victim computers, and which would thereby damage, and otherwise provide unauthorized access to, protected computers belonging to victims.

24. As part of the conspiracy, the Computer Hacking Conspirators, in some instances, engaged in “supply chain attacks.” In a “supply chain attack,” Computer Hacking Conspirators would gain unauthorized access to a victim software company’s computer network and modify the software company’s otherwise legitimate software with malicious code. The victim software company – unaware of the malicious changes to its product – would subsequently distribute the modified software to its third-party customers, who were thereby defrauded into installing malicious software code on their own computers. The Computer Hacking Conspirators could then leverage that malicious code to further damage, and to obtain information from, those computers.

25. As part of the conspiracy, the Computer Hacking Conspirators registered and used malicious and deceptive web domains that fraudulently incorporated or mimicked the names of prominent companies (*e.g.*, Google and Microsoft) in the domain names, for the purpose of avoiding detection by tricking targeted victims, cybersecurity professionals, and cybersecurity systems into believing that Internet traffic associated with those domains was legitimate or otherwise innocent. These domains could then be used as command and control web domains (or

“C2 Domains”) for the purpose of controlling malware illicitly placed on protected computers belonging to victims.

26. As part of the conspiracy, the Computer Hacking 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 host malicious C2 Domains (as “C2 servers” for those C2 Domains), to send commands to (and receive information of value 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.

27. As part of the conspiracy, the Computer Hacking Conspirators created “C2 dead drops,” whereby the Computer Hacking Conspirators’ malware was programmed to contact conspirator-registered accounts on publicly-available web pages that were encoded with the IP addresses of C2 servers. Specifically, the dead drop pages included what might appear to be random strings of text, but the relevant malware was programmed to recognize the text strings (which typically started and/or ended with pre-programmed “anchor text”) and convert them into Computer Hacking Conspirator-controlled IP addresses or C2 domains. The malware would then cause the victim computers to communicate with the servers hosting those IP addresses or C2 domains.

28. As part of the conspiracy, the Computer Hacking 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 companies.

Overt Acts

29. In furtherance of the conspiracy, the following overt acts were committed 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:

- a. On or about May 12, 2011, and continuing until at least about November 9, 2016, a lease was obtained for HOP POINT ONE. HOP POINT ONE was used as a C2 server and to access online accounts controlled by the conspirators.
- b. On or about August 2, 2011, ACCOUNT ONE, was registered with an e-mail provider. This account was used for communications in furtherance of computer hacking, and to register additional criminal infrastructure.
- c. On or about August 17, 2011, ACCOUNT TWO, was registered with an e-mail provider. This account was used for communications in furtherance of computer hacking.
- d. During the course of the conspiracy, and continuing until at least August 11, 2014, WEB DOMAIN ONE, was maintained and used in connection with malware, including as a C2 domain for malware.

- e. Beginning on or about November 11, 2011, and continuing until about November 10, 2014, WEB DOMAIN TWO, was registered and used in connection with malware, including as a C2 domain for malware.
- f. On or about May 2, 2012, the e-mail account hostay88@gmail.com was registered with an e-mail provider. This account was used for communications in furtherance of computer hacking, for storing malware files, and for registering additional criminal infrastructure.
- g. On or about May 5, 2012, ACCOUNT THREE, was registered with an e-mail provider. This account was used to register additional accounts, and also to send spear-phishing e-mails.
- h. On or about December 4, 2013, ACCOUNT THREE sent a fraudulent spear-phishing e-mail to employees of VICTIM A.
- i. On or about September 26, 2014, the e-mail account metasploit3@gmail.com communicated with a domain name registrar, in an effort to regain access to C2 Domains which had been disabled.
- j. Between about November 2014 and about March 2015, DOMAIN REGISTRAR ACCOUNT ONE was used to control the Domain Name Services, that is, to designate the Internet Protocol (“IP”) address for, WEB DOMAIN THREE.
- k. On or about May 5, 2015, ACCOUNT FOUR was registered with an e-mail provider. This account was used for sending spear-phishing e-mails.

- l. On or about May 15, 2015, WEB DOMAIN FOUR, which would serve as a malicious C2 Domain, was registered with a domain name registrar.
- m. On or about October 17, 2016, ACCOUNT THREE was used to send fraudulent spear-phishing e-mails to employees of VICTIM A in New York. The spear-phishing e-mails contained malware that was configured to work with a C2 dead drop which was controlled by an account registered using HOP POINT ONE.

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

COUNT TWO

(Conspiracy to Commit Wire Fraud – Computer Hacking Conspiracy)

30. Paragraphs 1 through 17 and 20 through 29 are re-alleged here.
31. Beginning no later than May 2011 and continuing at least until November 2018, 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, ZHANG HAORAN, TAN DAILIN, and other Computer Hacking Conspirators unlawfully, knowingly, and willfully conspired, combined, confederated, and agreed, as set forth in Paragraphs 20 to 29, to commit wire fraud, that is, to devise, execute, and attempt to execute a scheme by means of false and fraudulent pretenses, representations, and promises, and to cause 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.

(Conspiracy, in violation of Title 18, United States Code, Sections 1349 and 1343)

COUNT THREE
**(Conspiracy to Cause Damage To and Obtain Unauthorized Access To Protected
Computers – Video Game Conspiracy)**

32. Paragraphs 1 through 17 are re-alleged here.

Overview of the Video Game Conspiracy

33. Beginning no later than November 2014, and continuing at least until November 2018, 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, ZHANG HAORAN, TAN DAILIN, and other Video Game Conspirators did knowingly and willfully combine, conspire, confederate, and agree with each other to commit the following offenses against the United States:

- a. 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, intentionally accessed, and attempted to access, computers without authorization, and thereby obtained, and attempted to obtain, information from protected computers belonging to video game companies and their employees, such conduct having involved an interstate and foreign communication, in violation of Title 18, United States Code, Sections 1030(a)(2) and (c)(2)(B)(i) and (ii); and
- 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 belonging to

video game companies and their employees, and caused, or attempted to cause, more than \$5,000 in 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);

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

Objects, Manners, and Means of the Video Game Conspiracy

34. The objects of the Video Game Conspiracy were to obtain and install malware on protected computers, to damage such computers, to gain unauthorized access to those and other protected computers owned or used by video game companies and their employees, to obtain information of value that belonged to the owners and users of the targeted protected computers, and to do so by means materially false and fraudulent representations and pretenses, and to otherwise defraud and obtain information and digital items of value, including gaming artifacts.

35. As part of the conspiracy, the Video Game Conspirators used the same manners and means which are described in Paragraphs 21 to 29, and which were used by the Computer Hacking Conspirators. The manners and means described in Paragraphs 21 to 29 are thus re-alleged here as part of the manners and means of the Video Game Conspiracy.

36. As part of the conspiracy, the Video Game Conspirators conspired, coordinated, and communicated with one another, and in combination with others, to obtain unauthorized access to computer networks belonging to video game companies. The Video Game Conspirators used that access, working together and in combination with others, to, among other things, fraudulently

obtain or generate gaming artifacts, monitor the efforts of victim companies to identify and thwart the Video Game Conspirators' activities, and to interfere with the efforts of other groups that were also seeking to illicitly obtain or generate gaming artifacts (*i.e.*, sabotaging their criminal competition).

37. As part of the conspiracy, the Video Game Conspirators coordinated and communicated with one another, and with others known and unknown to the Grand Jury, to sell illegally-obtained gaming artifacts for a profit.

Overt Acts

38. In furtherance of the conspiracy, the following overt acts were committed 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:

- a. On or about November 26, 2014, malware was installed on protected computers at VICTIM B, including malware that provided the Video Game Conspirators unauthorized access to, and information from, protected computers belonging to VICTIM B.
- b. On or about December 9, 2014, malware installed on protected computers at VICTIM B caused said computers to communicate, by means of interstate wire communications, with a C2 Server for the malware.
- c. On or about February 24, 2015, in furtherance of the Video Game Conspiracy, money was transferred into a bank account held at a bank in the PRC.

- d. On or about May 19, 2015, ACCOUNT FOUR sent more than ten fraudulent spear-phishing e-mails to employees of VICTIM B and other video-game related companies.
- e. On or about March 24, 2016, ACCOUNT FIVE sent a file containing IP addresses and other information concerning a targeted video game company to ACCOUNT SIX.
- f. On or about May 9, 2016, ACCOUNT SEVEN sent fraudulent spear-phishing e-mails to a personal e-mail account of VICTIM C, and to the personal e-mail accounts of more than ten other individuals, including individuals in the video game industry.
- g. On or about June 15, 2016, HOP POINT TWO was used as a C2 server for malware installed at VICTIM D. The malware communicated with HOP POINT TWO by means of interstate wire communications.
- h. On or about June 25, 2016, login credentials belonging to J.L., an employee of VICTIM D, were used in furtherance of computer hacking and the wire fraud scheme.
- i. On or about June 22, 2016, \$362.85 was transmitted, transported, and transferred from the PRC to the United States, as payment for the lease of HOP POINT ONE.
- j. On or about August 20, 2016, ACCOUNT EIGHT sent Visa gift card information to ACCOUNT FIVE. The gift cards, which were registered

with fraudulent mailing addresses, were later used in attempted credit card transactions with a social media company.

- k. On or about October 17, 2016, spear-phishing e-mails were sent to computers belonging to VICTIM A, by means of wires in interstate and foreign commerce.
- l. On or about February 27, 2017, malware was installed on a protected computer belonging to VICTIM E. The malware was configured to, and did, communicate with WEB DOMAIN FOUR as its C2 Domain, thereby sending the C2 Server information from protected computers belonging to VICTIM E.
- m. On or about February 27, 2017, ACCOUNT EIGHT sent a file containing IP addresses and other information concerning a targeted video game company to ACCOUNT FIVE.
- n. On or about March 21, 2017, in an attempt to install malware and thereby cause damage to protected computers, fraudulent spear-phishing e-mails were sent to VICTIM D.
- o. On or about October 17, 2017, ACCOUNT NINE sent fraudulent spear-phishing e-mails to more than ten employees of VICTIM A.
- p. On or about October 19, 2017, ACCOUNT TEN discussed with ACCOUNT ELEVEN a refund request from a customer whose accounts were “shut down” by a video game company, after the customer purchased fraudulently-obtained gaming artifacts from the Video Game Conspirators.

- q. On or about February 18, 2018, ACCOUNT TEN discussed with ACCOUNT TWELVE possible international travel for the purpose of obtaining a private bank account in which to deposit the proceeds of the Video Game Conspiracy. ACCOUNT TWELVE expressed fear that “the Americans are after me” and that the Americans “have stuff on us.” ACCOUNT TEN suggested obtaining fake identification documents.
- r. On or about February 23, 2018, ACCOUNT TEN discussed with ACCOUNT ELEVEN the procedures that should be used to maximize profit in the sale of gaming artifacts, while avoiding detection by the relevant video game company.
- s. On or about March 11, 2018, ACCOUNT TEN told ACCOUNT ELEVEN that the conspirators were the only group with “illegal goods” in one particular region.
- t. During 2018, the conspirators obtained use of HOP POINT THREE, a computer server located outside of the United States, for the purpose of accessing spear-phishing e-mail accounts and other online accounts, by means of wire communications.
- u. On or about June 18, 2018, using a means of identification belonging to VICTIM C, HOP POINT THREE was used to gain unauthorized access to, and to obtain information from, an e-mail account belonging to VICTIM C.
- v. During August 2018, WEB DOMAIN FIVE was registered using HOP POINT THREE.

- w. During August 2018, access was obtained to HOP POINT FOUR, which was used as a C2 server.
- x. On or about November 16, 2018, VICTIM F installed what appeared to be legitimate software onto one of its Internet-connected computers in California. VICTIM F obtained the software from a legitimate provider. Unbeknownst to VICTIM F, as a part of the Video Game Conspiracy, and by means of a supply chain attack, the Video Game Conspirators had earlier fraudulently modified the software installed by VICTIM F, such that it included malicious code within the otherwise-legitimate software package.
- y. Shortly after installation, the malicious code caused VICTIM F's computer, to engage in wire communications with a subdomain of WEB DOMAIN FIVE, which then resolved to HOP POINT FOUR.
- z. As a result, between about November 16, 2018, and about November 20, 2018, unauthorized access was obtained to protected computers belonging to VICTIM F, and that access was used to obtain information, including information about VICTIM F's computer network.

39. The malware installed on computers belonging to VICTIMS B, D, E, and F caused losses exceeding \$5,000 for each of VICTIMS B, D, E, and F.

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

COUNT FOUR

(Conspiracy to Commit Wire Fraud – Video Game Conspiracy)

40. Paragraphs 1 through 17 and 34 through 39 are re-alleged here.

41. Beginning no later than November 2014, and continuing at least until November 2018, 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, ZHANG HAORAN, TAN DAILIN and other Video Game Conspirators unlawfully, knowingly, and willfully conspired, combined, confederated, and agreed, as set forth in Paragraphs 34 to 39, to commit wire fraud, that is, to devise, execute, and attempt to execute a scheme by means of false and fraudulent pretenses, representations, and promises, and to cause 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.

(**Conspiracy**, in violation of Title 18, United States Code, Sections 1349 and 1343)

COUNT FIVE
(Wire Fraud)

42. Paragraphs 1 through 17 and 20 through 29 are re-alleged here.

43. Beginning no later than May 2011, and continuing at least until November 2018, 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, ZHANG HAORAN, TAN DAILIN, and other Computer Hacking Conspirators, with intent to defraud, knowingly devised and intended to devise a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, to obtain information by unauthorized access to protected computers, including by means of false and fraudulent representations, and pretenses, and executed through interstate and foreign wire communications, as set forth in Paragraphs 20 to 29.

44. On or about September 26, 2014, for the purpose of executing the scheme and artifice to defraud, and attempting to do so, ZHANG HAORAN, TAN DAILIN, and other Computer Hacking Conspirators did transmit and cause to be transmitted, by means of wire communications in interstate and foreign commerce between a computer in the PRC and computers in the State of Washington, writings, signs, and signals, which consisted of an e-mail from metasploit3@gmail.com to a Domain Name Registrar, in an effort to regain access to C2 Domains which had been disabled by the Domain Name Registrar.

(Wire Fraud, in violation of Title 18, United States Code, Section 1343)

COUNT SIX

(Intentional Damage to a Protected Computer of Victim B)

45. Paragraphs 1 through 17 and 34 through 39 are re-alleged here.

46. On or about November 26, 2014, 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, ZHANG HAORAN, TAN DAILIN, and other Video Game Conspirators 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 VICTIM B, and thereby would and did intentionally cause loss to one or more persons during 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.

(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 SEVEN

(Obtaining Information by Unauthorized Access to Protected Computers of Victim B)

47. Paragraphs 1 through 17 and 34 through 39 are re-alleged here.

48. On or about November 26, 2014, 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, ZHANG HAORAN, TAN DAILIN, and other Video Game Conspirators attempted to intentionally access, and did intentionally access, a protected computer without authorization, and thereby obtained information from a protected computer belonging to VICTIM B.

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

COUNT EIGHT

(Wire Fraud – Victim B)

49. Paragraphs 1 through 17 and 34 through 39 are re-alleged here.

50. Beginning no later than November 2014, and continuing at least until November 2018, 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, ZHANG HAORAN, TAN DAILIN, and other Video Game Conspirators, with intent to defraud, knowingly devised and intended to devise a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, to obtain information by unauthorized access to protected computers,

including by means of false and fraudulent representations, and pretenses, and executed through interstate and foreign wire communications, as set forth in Paragraphs 34 to 39.

51. On or about December 9, 2014, for the purpose of executing the scheme and artifice to defraud, and attempting to do so, ZHANG HAORAN, TAN DAILIN, and other Video Game Conspirators did transmit and cause to be transmitted, by means of wire communications in interstate and foreign commerce between the State of California and the State of Texas, writings, signs, and signals which comprised communications exchanging electronic information between a computer belonging to VICTIM B and a C2 server in California.

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

COUNT NINE

(Attempted Intentional Damage to a Protected Computer of Victim B)

52. Paragraphs 1 through 17 and 34 through 39 are re-alleged here.

53. On or about May 19, 2015, 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, ZHANG HAORAN, TAN DAILIN, and other Video Game Conspirators knowingly attempted to cause, and did cause, the transmission of a program, information, code, and command, and, through such conduct, attempted to intentionally cause damage without authorization to protected computers belonging to VICTIM B, which damage, if completed, would have caused loss to one or more persons during one-year period from the defendants' course of conduct affecting protected computers aggregating at least \$5,000 in

value, and, if completed, the defendants' course of conduct would have affected 10 or more protected computers during a one-year period.

(Attempted 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 TEN

(Intentional Damage to a Protected Computer of Victim D)

54. Paragraphs 1 through 17 and 34 through 39 are re-alleged here.

55. On or about June 15, 2016, 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, ZHANG HAORAN, TAN DAILIN, and other Video Game Conspirators 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 VICTIM D, and thereby caused loss to one or more persons during 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.

(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 ELEVEN

(Obtaining Information by Unauthorized Access to Protected Computers of Victim D)

56. Paragraphs 1 through 17 and 34 through 39 are re-alleged here.

57. On or about June 15, 2016, 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, ZHANG HAORAN, TAN DAILIN, and other Video Game Conspirators attempted to intentionally access, and did intentionally access, a protected computer without authorization, and thereby obtained information from a protected computer belonging to VICTIM D.

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

COUNT TWELVE
(Aggravated Identity Theft – Employee of Victim D)

58. Paragraphs 1 through 17 and 34 through 39 are re-alleged here.

59. On or about June 25, 2016, 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 Unauthorized Access to Protected Computers, in violation of Title 18, United States Code, Section 1030(a)(2), ZHANG HAORAN, TAN DAILIN, and other Video Game Conspirators did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, namely, J.L., an employee of VICTIM D.

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

COUNT THIRTEEN
(Wire Fraud – Victim D)

60. Paragraphs 1 through 17 and 34 through 39 are re-alleged here.

61. Beginning no later than November 2014, and continuing at least until November 2018, 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, ZHANG HAORAN, TAN DAILIN, and other Video Game Conspirators, with intent to defraud, knowingly devised and intended to devise a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, to obtain information by unauthorized access to protected computers, including by means of false and fraudulent representations, and pretenses, and executed through interstate and foreign wire communications, as set forth in Paragraphs 34 to 39.

62. On or about June 15, 2016, for the purpose of executing the scheme and artifice to defraud, and attempting to do so, ZHANG HAORAN, TAN DAILIN, and other Video Game Conspirators did transmit and cause to be transmitted, by means of wire communications in interstate and foreign commerce between the State of California and the State of Washington, writings, signs, and signals which comprised communications exchanging electronic information between a computer belonging to VICTIM D and HOP POINT TWO.

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

COUNT FOURTEEN
(Money Laundering)

63. Paragraphs 1 through 17, 20 through 29, and 34 through 39 are re-alleged here.

64. On or about June 22, 2016, 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, ZHANG HAORAN, TAN DAILIN, and other Video Game Conspirators knowingly transported, transmitted, and transferred funds, and aided, abetted and willfully caused, the transport, transmitting, and transfer of funds, that is, a \$362.85 payment for the lease of HOP POINT ONE, 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), 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)

COUNT FIFTEEN

(Attempted Intentional Damage to a Protected Computer of Victim A)

65. Paragraphs 1 through 17 and 34 through 39 are re-alleged here.

66. On or about October 17, 2016, 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, ZHANG HAORAN, TAN DAILIN, and other Video Game Conspirators knowingly attempted to cause, and did cause, the transmission of a program, information, code, and command, and, through such conduct, attempted to intentionally cause damage without authorization to protected computers belonging to VICTIM A, which damage, if completed, would have caused loss to one or more persons during one-year period from the defendants' course of conduct affecting protected computers aggregating at least \$5,000 in value, and, if completed, the defendants' course of conduct would have affected 10 or more protected computers during a one-year period.

(Attempted 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 SIXTEEN

(Wire Fraud – Victim A)

67. Paragraphs 1 through 17 and 34 through 39 are re-alleged here.

68. Beginning no later than November 2014, and continuing at least until November 2018, 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, ZHANG HAORAN, TAN DAILIN, and other Video Game Conspirators, with intent to defraud, knowingly devised and intended to devise a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, to obtain information by unauthorized access to protected computers, including by means of false and fraudulent representations, and pretenses, and executed through interstate and foreign wire communications, as set forth in Paragraphs 34 to 39.

69. On or about October 17, 2016, for the purpose of executing the scheme and artifice to defraud, and attempting to do so, ZHANG HAORAN, TAN DAILIN, and other Video Game Conspirators did transmit and cause to be transmitted, by means of wire communications in interstate and foreign commerce between Taiwan and the State of New York, writings, signs, and signals which comprised communications exchanging electronic information between HOP POINT ONE and a computer belonging to VICTIM A.

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

COUNT SEVENTEEN

(Attempted Intentional Damage to a Protected Computer of Victim C)

70. Paragraphs 1 through 17 and 34 through 39 are re-alleged here.

71. On or about May 9, 2016, 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, ZHANG HAORAN, TAN DAILIN, and other Video Game Conspirators knowingly attempted to cause, and did cause, the transmission of

a program, information, code, and command, and, through such conduct, attempted to intentionally cause damage without authorization to protected computers belonging to VICTIM C, and, if completed, the defendants' course of conduct would have affected 10 or more protected computers during a one-year period.

(Attempted 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 EIGHTEEN

(Intentional Damage to a Protected Computer of Victim E)

72. Paragraphs 1 through 17 and 34 through 39 are re-alleged here.

73. On or about February 27, 2017, 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, ZHANG HAORAN, TAN DAILIN, and other Video Game Conspirators 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 VICTIM E, which damage caused loss to one or more persons during one-year period from the defendants' course of conduct affecting protected computers aggregating at least \$5,000 in value, and the defendants' course of conduct affected 10 or more protected computers during a one-year period.

(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 NINETEEN

(Obtaining Information by Unauthorized Access to Protected Computers of Victim E)

74. Paragraphs 1 through 17 and 34 through 39 are re-alleged here.

75. On or about February 27, 2017, 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, ZHANG HAORAN, TAN DAILIN, and other Video Game Conspirators attempted to intentionally access, and did intentionally access, a protected computer without authorization, and thereby obtained information from a protected computer belonging to VICTIM E

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

COUNT TWENTY

(Attempted Intentional Damage to a Protected Computer of Victim D)

76. Paragraphs 1 through 17 and 34 through 39 are re-alleged here.

77. On or about March 21, 2017, 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, ZHANG HAORAN, TAN DAILIN, and other Video Game Conspirators knowingly attempted to cause, and did cause, the transmission of a program, information, code, and command, and, through such conduct, attempted to intentionally cause damage without authorization to protected computers belonging to VICTIM D, which damage, if completed, would have caused loss to one or more persons during one-year period from the defendants' course of conduct affecting protected computers aggregating at least

\$5,000 in value, and, if completed, the defendants' course of conduct would have affected 10 or more protected computers during a one-year period.

(Attempted 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-ONE

(Attempted Intentional Damage to a Protected Computer of Victim A)

78. Paragraphs 1 through 17 and 34 through 39 are re-alleged here.

79. On or about August 4, 2017, 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, ZHANG HAORAN, TAN DAILIN, and other Video Game Conspirators knowingly attempted to cause, and did cause, the transmission of a program, information, code, and command, and, through such conduct, attempted to intentionally cause damage without authorization to protected computers belonging to VICTIM A, which damage, if completed, would have caused loss to one or more persons during one-year period from the defendants' course of conduct affecting protected computers aggregating at least \$5,000 in value, and, if completed, the defendants' course of conduct would have affected 10 or more protected computers during a one-year period.

(Attempted 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-TWO

(Aggravated Identity Theft – Victim C)

80. Paragraphs 1 through 17 and 34 through 39 are re-alleged here.

81. On or about June 18, 2018, during and in relation to the crime of Obtaining Information by Unauthorized Access to Protected Computers, in violation of Title 18, United States

Code, Section 1030(a)(2), ZHANG HAORAN, TAN DAILIN, and other Video Game Conspirators did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, namely, 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-THREE
(Intentional Damage to a Protected Computer of Victim F)

82. Paragraphs 1 through 17 and 34 through 39 are re-alleged here.

83. On or about November 16, 2018, 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, ZHANG HAORAN, TAN DAILIN, and other Video Game Conspirators 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 VICTIM F, which damage caused loss to one or more persons during one-year period from the defendants' course of conduct affecting protected computers aggregating at least \$5,000 in value, and the defendants' course of conduct affected 10 or more protected computers during a one-year period.

(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-FOUR
(Obtaining Information by Unauthorized Access to Protected Computers of Victim F)

84. Paragraphs 1 through 17 and 34 through 39 are re-alleged here.

85. On or about November 16, 2018, 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, ZHANG HAORAN, TAN DAILIN, and other Video Game Conspirators attempted to intentionally access, and did intentionally access, a protected computer without authorization, and thereby obtained information from a protected computer belonging to VICTIM F.

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

COUNT TWENTY-FIVE
(Wire Fraud – Victim F)

86. Paragraphs 1 through 17 and 34 through 39 are re-alleged here.

87. Beginning no later than November 2014, and continuing at least until November 2018, 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, ZHANG HAORAN, TAN DAILIN, and other Video Game Conspirators, with intent to defraud, knowingly devised and intended to devise a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, to obtain information by unauthorized access to protected computers, including by means of false and fraudulent representations, and pretenses, and executed through interstate and foreign wire communications, as set forth in Paragraphs 34 to 39.

88. On or about November 16, 2018, for the purpose of executing the scheme and artifice to defraud, and attempting to do so, ZHANG HAORAN, TAN DAILIN, and other Video

Game Conspirators did transmit and cause to be transmitted, by means of wire communications in interstate and foreign commerce between the State of California and the State of New York, writings, signs, and signals which comprised communications exchanging electronic information between a computer belonging to VICTIM F and HOP POINT FOUR.

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

FORFEITURE ALLEGATION

1. Upon conviction of any of the offenses alleged in Counts 1, 3, 5, 8, 13, 16, and/or 25 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, 3, 6, 7, 9, 10, 11, 15, 17, 18, 19, 20, 21, 23, and/or 24 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 personal 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, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 13, 15, 16, 17, 18, 19, 20, 21, 23, 24 and/or 25 of this Indictment, the defendants 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 defendants 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 14 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;

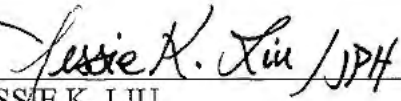
the defendant shall forfeit to the United States any other property of the defendant, up to the value of the property described above, pursuant to 21 U.S.C. § 853(p).

(Criminal Forfeiture, pursuant to Title 18, United States Code, Section 981(a)(1)(C),

Title 28, United States 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



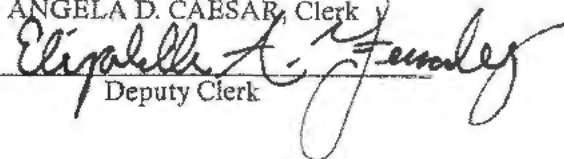
JESSIE K. LIU
UNITED STATES ATTORNEY IN AND FOR
THE DISTRICT OF COLUMBIA

U.S. District and Bankruptcy Courts
for the District of Columbia

A TRUE COPY

ANGELA D. CAESAR, Clerk

By



Deputy Clerk