

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

USDC SDNY
DOCUMENT
ELECTRONICALLY FILED
DOC #:
DATE FILED: **DEC 17 2018**

- - - - - x
:
UNITED STATES OF AMERICA :
:
-v.- :
:
ZHU HUA, :
a/k/a "Afwar," :
a/k/a "CVNX," :
a/k/a "Alayos," :
a/k/a "Godkiller," and :
ZHANG SHILONG, :
a/k/a "Baobeilong," :
a/k/a "Zhang Jianguo," :
a/k/a "Atreexp," :
:
Defendants. :
:
- - - - - x

SEALED INDICTMENT

18 Cr. _____

18 CRIM 891

COUNT ONE
(Conspiracy to Commit Computer Intrusions)

The Grand Jury charges:

OVERVIEW

1. At all times relevant to this Indictment, ZHU HUA (朱华), a/k/a "Afwar," a/k/a "CVNX," a/k/a "Alayos," a/k/a "Godkiller," and ZHANG SHILONG (张士龙), a/k/a "Baobeilong," a/k/a "Zhang Jianguo," a/k/a "Atreexp," the defendants, both of whom were nationals of the People's Republic of China ("China"), were members of a hacking group operating in China known within the cyber security community as Advanced Persistent Threat 10

(the "APT10 Group")¹, or alternatively as "Red Apollo," "CVNX," "Stone Panda," "MenuPass," and "POTASSIUM."

2. From at least in or about 2006 up to and including in or about 2018, members of the APT10 Group, including ZHU HUA, a/k/a "Afwar," a/k/a "CVNX," a/k/a "Alayos," a/k/a "Godkiller," and ZHANG SHILONG, a/k/a "Baobeilong," a/k/a "Zhang Jianguo," a/k/a "Atreexp," the defendants, conducted extensive campaigns of global intrusions into computer systems. The defendants worked for Huaying Haitai Science and Technology Development Company ("Huaying Haitai") in Tianjin, China, and acted in association with the Chinese Ministry of State Security's Tianjin State Security Bureau.

3. While the APT10 Group employed similar hacking tools and techniques over the course of its campaigns, the APT10 Group's hacking operations evolved over time, demonstrating advances in overcoming network defenses, victim selection, and tradecraft. Moreover, the APT10 Group utilized some of the same online facilities to initiate, facilitate, and execute its

¹ APT is a designation given in the cyber security community to an individual or group that uses sophisticated techniques to exploit vulnerabilities in victim computer systems and employs an external command and control system to target a specific entity or range of entities and maintain a persistent presence on its targets' networks.

campaigns during the conspiracy, thereby reflecting the APT10 Group's continuous and unrelenting effort, from in or about 2006 up to and including in or about 2018, to steal technologies and other information of value to the conspiracy. For example, as detailed herein, the APT10 Group was engaged in at least two computer intrusion campaigns during the relevant time period, both aiming to steal, among other data, intellectual property and confidential business or technological information:

a. First, beginning in or about 2006, members of the APT10 Group, including ZHU HUA, a/k/a "Afwar," a/k/a "CVNX," a/k/a "Alayos," a/k/a "Godkiller," and ZHANG SHILONG, a/k/a "Baobeilong," a/k/a "Zhang Jianguo," a/k/a "Atreexp," the defendants, engaged in an intrusion campaign to obtain unauthorized access to the computers and computer networks of commercial and defense technology companies and U.S. Government agencies in order to steal information and data concerning a number of technologies (the "Technology Theft Campaign"). Specifically, the APT10 Group obtained unauthorized access to the computers of more than 45 such entities based in at least 12 states, including Arizona, California, Connecticut, Florida, Maryland, New York, Ohio, Pennsylvania, Texas, Utah, Virginia, and Wisconsin. Through the Technology Theft Campaign, the APT10

Group stole hundreds of gigabytes of sensitive data and targeted the computers of victim companies involved in a diverse array of commercial activity, industries, and technologies, including aviation, space and satellite technology, manufacturing technology, pharmaceutical technology, oil and gas exploration and production technology, communications technology, computer processor technology, and maritime technology.

b. Second, beginning at least in or about 2014, members of the APT10 Group, including ZHU and ZHANG, engaged in an intrusion campaign to obtain unauthorized access to the computers and computer networks of managed service providers ("MSPs") for businesses and governments around the world (the "MSP Theft Campaign"). MSPs are companies that remotely manage their clients' information technology infrastructure, including by providing computer servers, storage, networking, consulting and information technology support. The APT10 Group targeted MSPs in order to leverage the MSPs' networks to gain unauthorized access to the computers and computer networks of the MSPs' clients and steal, among other data, intellectual property and confidential business data on a global scale. For example, through the MSP Theft Campaign, the APT10 Group obtained unauthorized access to the computers of an MSP that had

offices in the Southern District of New York and compromised the data of that MSP and certain of its clients located in at least 12 countries, including Brazil, Canada, Finland, France, Germany, India, Japan, Sweden, Switzerland, the United Arab Emirates, the United Kingdom, and the United States. Those compromised clients included companies that were involved in a diverse array of commercial activity, industries, and technologies, including banking and finance, telecommunications and consumer electronics, medical equipment, packaging, manufacturing, consulting, healthcare, biotechnology, automotive, oil and gas exploration, and mining.

c. In addition, the APT10 Group compromised more than 40 computers in order to steal confidential data from those systems belonging to the United States Department of the Navy (the "Navy"), including the personally identifiable information of more than 100,000 Navy personnel.

MEANS AND METHODS OF THE CONSPIRACY

The Technology Theft Campaign

4. Members of the APT10 Group, including ZHU HUA, a/k/a "Afwar," a/k/a "CVNX," a/k/a "Alayos," a/k/a "Godkiller," and ZHANG SHILONG, a/k/a "Baobeilong," a/k/a "Zhang Jianguo," a/k/a "Atreexp," the defendants, engaged in the following stages of

activity to orchestrate and manage the computer intrusions committed during the Technology Theft Campaign, which are generally summarized below:

a. First, members of the APT10 Group used a technique known as "spear phishing" to introduce malicious software ("malware") onto targeted computers. Members of the conspiracy sent customized emails to intended targets with attached documents and files that would surreptitiously install malware if opened. In order to trick the recipients of the spear phishing emails into opening the attachments of the emails that installed the malware, the emails purported to be sent from legitimate email addresses, when in fact the emails were sent by members of the conspiracy. In addition, the content of the email messages and the filenames of the attachments appeared to be legitimate and contain information of interest to the recipients. For example, one spear phishing email purported to originate from an email address associated with a victim company ("Victim-1") involved in communications technology, when it actually originated from a different account, which was unaffiliated with Victim-1 and logged in from a computer

assigned an Internet protocol ("IP") address² located in Tianjin, China under the control of the APT10 Group. That email, which was sent to employees of another victim company ("Victim-2") involved in helicopter manufacturing, had the subject line "C17 Antenna problems," a malicious Microsoft Word attachment named "12-204 Side Load Testing.doc," and stated the following: "Please see the attached the files." When the attachment named "12-204 Side Load Testing.doc" was opened, malware was installed on the computer of Victim-2. By using these spear phishing methods, the conspirators intended to and did cause the recipients of the emails to open the attachments without arousing suspicion as to the source of the email or its attachments.

b. Second, once a recipient of a spear phishing email opened the attachment to the email, the attachment installed malware on the victim's computer. The malware typically included customized variants of a remote access Trojan ("RAT") including one known as "Poison Ivy" and keystroke loggers, which are programs that surreptitiously recorded

² Each electronic device or computer resource connected to the Internet must be assigned a unique IP address so that communications from or directed to that electronic device are routed properly.

computer keystrokes to steal usernames and passwords as the user of the victim systems typed them. The malware was programmed to automatically communicate with domains that were assigned IP addresses of computers under the control of members of the APT10 Group, allowing them to maintain visibility and persistent remote access to the compromised computers over the Internet. In particular, the APT10 Group used dynamic Domain Name System ("DNS") service providers to host their malicious domains, including a provider located in the Southern District of New York, which allowed the APT10 Group to route the pre-programmed malicious domains in their malware to different IP addresses of computers under their control. This mode of operation enabled the APT10 Group to frequently and rapidly change the IP addresses associated with their malicious domains without having to adjust the malware or domains already on a victim's computers, providing the APT10 Group with operational flexibility and persistence, as well as helping them avoid detection by bypassing network security filters that might block identified malicious IP addresses.

c. Third, after the malware was successfully installed, the APT10 Group downloaded additional malware and

tools to compromised computer systems in order to further compromise the victim's computers.

d. Fourth, after the APT10 Group had gained unauthorized access to a victim's computers and identified data of interest on those computers, the APT10 Group collected the relevant files and other information from the compromised computers and exfiltrated the stolen files and information in encrypted archives to computers under their control.

5. Over the course of the Technology Theft Campaign, the defendants and their coconspirators successfully obtained unauthorized access to at least approximately 90 computers belonging to, among others, commercial and defense technology companies and U.S. Government agencies located in at least 12 states, and stole hundreds of gigabytes of sensitive data and information from their computer systems, including from at least the following victims:

a. seven companies involved in aviation, space and/or satellite technology;

b. three companies involved in communications technology;

- c. three companies involved in manufacturing advanced electronic systems and/or laboratory analytical instruments;
- d. a company involved in maritime technology;
- e. a company involved in oil and gas drilling, production, and processing;
- f. The National Aeronautics and Space Administration ("NASA") Goddard Space Center; and
- g. The NASA Jet Propulsion Laboratory.

6. In addition to the above victims, the defendants and their coconspirators successfully obtained unauthorized access to computers belonging to at least 25 other technology-related companies involved in, among other things, industrial factory automation, radar technology, oil exploration, information technology services, pharmaceutical manufacturing, and computer processor technology, as well as the U.S. Department of Energy's Lawrence Berkeley National Laboratory.

The MSP Theft Campaign

7. In order to conduct the MSP Theft Campaign, members of the APT10 Group, including ZHU HUA, a/k/a "Afwar," a/k/a "CVNX," a/k/a "Alayos," a/k/a "Godkiller," and ZHANG SHILONG, a/k/a "Baobeilong," a/k/a "Zhang Jianguo," a/k/a "Atreexp," the

defendants, generally engaged in the same stages of activity involved in the Technology Theft Campaign as set forth above in paragraph 4. In addition, the APT10 Group engaged in the following conduct related to the MSP Theft Campaign:

a. After the APT10 Group had gained unauthorized access into the computers of an MSP, the APT10 Group installed multiple different customized variants of malware commonly known as PlugX, RedLeaves, and QuasarRAT on MSP computers located around the world. The malware was installed using malicious files that masqueraded as legitimate files used by a victim computer's operating system in order to mask the APT10 Group's actions as legitimate and thereby avoid antivirus detection. Such malware enabled members of the APT10 Group to monitor victims' computers remotely and steal user credentials using various credential theft tools. The malware was also pre-programmed to automatically communicate with domains hosted by DNS service providers that were assigned IP addresses of computers under the control of the APT10 Group. In total, the APT10 Group registered approximately 1,300 unique malicious domains in connection with the MSP Theft Campaign, some of which were registered using accounts opened as early as in or about 2010.

b. Once the APT10 Group had stolen administrative credentials from computers of an MSP, it used those stolen credentials to initiate Remote Desktop Protocol ("RDP") connections to other systems within an MSP and its clients' networks. This mode of operation enabled the APT10 Group to move laterally through the interconnected networks of an MSP and its clients' networks and to compromise an MSP and its clients' computers on which no malware had been previously installed.

c. Finally, after data of interest was identified on a compromised computer and packaged for exfiltration using encrypted archives, the APT10 Group often used stolen credentials to move the data of an MSP client to one or more other compromised computers of the MSP or its other clients' networks before the final exfiltration of the data to IP addresses under the control of the APT10 Group. The APT10 Group usually deleted the stolen files from compromised computers, thereby seeking to avoid detection and preventing identification of the specific files that were stolen.

8. Throughout the conspiracy period, after the U.S. Government or certain private sector firms issued various public reports identifying APT10 Group malware or domains as malicious, the APT10 Group modified or abandoned such hacking

infrastructure. For example, in or about February 2007 during the Technology Theft Campaign, InfraGard, a non-profit organization serving as a public-private partnership between U.S. businesses and the Federal Bureau of Investigation, issued a public report identifying the malicious domains used by the APT10 Group. Shortly after the Infragard report's release, the APT10 Group stopped using the malicious domains identified in the report. Similarly, in or about April 2017 during the MSP Theft Campaign, a private cyber security firm issued a public report identifying the malicious domains used by the APT10 Group. Shortly after the report was issued, the APT10 Group began using new variants of malware and new domains to commit intrusions, which would be less likely to be detected by victim companies and antivirus software.

9. Over the course of the MSP Theft Campaign, members of the APT10 Group, including ZHU HUA, a/k/a "Afwar," a/k/a "CVNX," a/k/a "Alayos," a/k/a "Godkiller," and ZHANG SHILONG, a/k/a "Baobeilong," a/k/a "Zhang Jianguo," a/k/a "Atreexp," the defendants, successfully obtained unauthorized access to computers providing services to or belonging to victim companies located in at least 12 countries, including from at least the following victims:

- a. a global financial institution;
- b. three telecommunications and/or consumer electronics companies;
- c. three companies involved in commercial or industrial manufacturing;
- d. two consulting companies;
- e. a healthcare company;
- f. a biotechnology company;
- g. a mining company;
- h. an automotive supplier company; and
- i. a drilling company.

10. Finally, the APT10 Group also compromised more than 40 computers in order to steal sensitive data belonging to the Navy, including the names, Social Security numbers, dates of birth, salary information, personal phone numbers, and email addresses of more than 100,000 Navy personnel.

The Defendants' Participation in the Hacking Campaigns

11. At all times relevant to this Indictment, the APT10 Group was a hacking group operating in Tianjin, China, among other places in China. The members of the APT10 Group worked in an office environment and typically engaged in hacking operations during working hours in China.

12. ZHU HUA, a/k/a "Afwar," a/k/a "CVNX," a/k/a "Alayos," a/k/a "Godkiller," the defendant, a penetration tester who worked for Huaying Haitai, registered malicious domains and hacking infrastructure used in connection with the APT10 Group's intrusion campaigns and engaged in hacking operations on behalf of the APT10 Group. ZHU was also involved in the recruitment of other individuals to the APT10 Group.

13. ZHANG SHILONG, a/k/a "Baobeilong," a/k/a "Zhang Jianguo," a/k/a "Atreexp," the defendant, who worked for Huaying Haitai, registered malicious domains and hacking infrastructure used in connection with the APT10 Group's intrusion campaigns. ZHANG also developed and tested malware used in connection with the APT10 Group's intrusion campaigns.

STATUTORY ALLEGATIONS

14. From at least in or about 2006 up to and including in or about 2018, in the Southern District of New York and elsewhere, ZHU HUA, a/k/a "Afwar," a/k/a "CVNX," a/k/a "Alayos," a/k/a "Godkiller," and ZHANG SHILONG, a/k/a "Baobeilong," a/k/a "Zhang Jianguo," a/k/a "Atreexp," the defendants, who will first be brought to the Southern District of New York, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit

computer intrusion offenses in violation of Title 18, United States Code, Sections 1030(a)(2)(C), 1030(c)(2)(B)(iii), 1030(a)(4), 1030(c)(3)(A), 1030(a)(5)(A), 1030(c)(4)(A)(i)(I) & (VI), and 1030(c)(4)(B)(i).

15. It was a part and an object of the conspiracy that ZHU HUA, a/k/a "Afwar," a/k/a "CVNX," a/k/a "Alayos," a/k/a "Godkiller," and ZHANG SHILONG, a/k/a "Baobeilong," a/k/a "Zhang Jianguo," a/k/a "Atreexp," the defendants, and others known and unknown, would and did intentionally access computers without authorization, and exceed authorized access, and thereby would and did obtain information from protected computers, and the value of the information obtained would and did exceed \$5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B)(iii).

16. It was further a part and an object of the conspiracy that ZHU HUA, a/k/a "Afwar," a/k/a "CVNX," a/k/a "Alayos," a/k/a "Godkiller," and ZHANG SHILONG, a/k/a "Baobeilong," a/k/a "Zhang Jianguo," a/k/a "Atreexp," the defendants, and others known and unknown, knowingly and with the intent to defraud, would and did access protected computers without authorization, and exceed authorized access, and by means of such conduct further the intended fraud and obtain anything of value, in violation of

Title 18, United States Code, Sections 1030(a)(4) and 1030(c)(3)(A).

17. It was further a part and an object of the conspiracy that ZHU HUA, a/k/a "Afwar," a/k/a "CVNX," a/k/a "Alayos," a/k/a "Godkiller," and ZHANG SHILONG, a/k/a "Baobeilong," a/k/a "Zhang Jianguo," a/k/a "Atreexp," the defendants, and others known and unknown, knowingly would and did cause the transmissions of programs, information, codes, and commands, and as a result of such conduct, intentionally caused damage without authorization to protected computers, which caused loss to one and more persons during any one-year period aggregating at least \$5,000 in value and damage affecting ten or more protected computers during any one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(A)(i)(I) & (VI), and 1030(c)(4)(B)(i).

(Title 18, United States Code, Sections 1030(b) and 3238.)

COUNT TWO
(Conspiracy to Commit Wire Fraud)

The Grand Jury further charges:

18. The allegations contained in paragraphs 1 through 13 of this Indictment are repeated and realleged as if fully set forth herein.

19. From at least in or about 2006 up to and including in or about 2018, in the Southern District of New York and elsewhere, ZHU HUA, a/k/a "Afwar," a/k/a "CVNX," a/k/a "Alayos," a/k/a "Godkiller," and ZHANG SHILONG, a/k/a "Baobeilong," a/k/a "Zhang Jianguo," a/k/a "Atreexp," the defendants, who will first be brought to the Southern District of New York, and others known and unknown, willfully and knowingly did combine, conspire, confederate, and agree together and with each other to commit wire fraud, in violation of Title 18, United States Code, Section 1343.

20. It was a part and object of the conspiracy that ZHU HUA, a/k/a "Afwar," a/k/a "CVNX," a/k/a "Alayos," a/k/a "Godkiller," and ZHANG SHILONG, a/k/a "Baobeilong," a/k/a "Zhang Jianguo," a/k/a "Atreexp," the defendants, and others known and unknown, willfully and knowingly, having devised and intending to devise a scheme and artifice to defraud and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, in violation of Title 18,

United States Code, Section 1343, to wit, ZHU and ZHANG engaged in a scheme together with others to fraudulently obtain intellectual property and confidential business or technological information from victim companies by remotely accessing through the Internet, and without authorization, the computers of the victims using stolen login credentials of victim employees.

(Title 18, United States Code, Sections 1349 and 3238.)

COUNT THREE
(Aggravated Identity Theft)

The Grand Jury further charges:

21. The allegations contained in paragraphs 1 through 13 of this Indictment are repeated and realleged as if fully set forth herein.

22. From at least in or about 2006 up to and including in or about 2018, in the Southern District of New York and elsewhere, ZHU HUA, a/k/a "Afwar," a/k/a "CVNX," a/k/a "Alayos," a/k/a "Godkiller," and ZHANG SHILONG, a/k/a "Baobeilong," a/k/a "Zhang Jianguo," a/k/a "Atreexp," the defendants, who will first be brought to the Southern District of New York, knowingly transferred, possessed, and used, without lawful authority, a means of identification of another person, during and in relation to a felony violation enumerated in Title 18, United States Code, Section 1028A(c), and aided and abetted the same,

to wit, ZHU and ZHANG transferred, possessed, and used, and aided and abetted the transfer, possession, and use of, the name of another person and login credentials including usernames and passwords of various employees of victims of computer intrusions during and in relation to the computer fraud and wire fraud offenses charged in Counts One and Two of this Indictment.

(Title 18, United States Code, Sections 1028A(a)(1) & (b),
3238, and 2.)

FORFEITURE ALLEGATION AS TO COUNT ONE

23. As a result of committing the offense alleged in Count One of this Indictment, ZHU HUA, a/k/a "Afwar," a/k/a "CVNX," a/k/a "Alayos," a/k/a "Godkiller," and ZHANG SHILONG, a/k/a "Baobeilong," a/k/a "Zhang Jianguo," a/k/a "Atreexp," the defendants, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 1030(i), any and all property, real and personal, constituting or derived from, any proceeds obtained directly or indirectly, as a result of said offense, and any and all personal property that was used or intended to be used to commit or to facilitate the commission of said offense, including but not limited to a sum of money in United States currency representing the amount of proceeds traceable to the commission of said offense.

FORFEITURE ALLEGATION AS TO COUNT TWO

24. As a result of committing the offense alleged in Count Two of this Indictment, ZHU HUA, a/k/a "Afwar," a/k/a "CVNX," a/k/a "Alayos," a/k/a "Godkiller," and ZHANG SHILONG, a/k/a "Baobeilong," a/k/a "Zhang Jianguo," a/k/a "Atreexp," the defendants, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C), and Title 28, United States Code, Section 2461(c), any and all property, real and personal, that constitutes or is derived from proceeds traceable to the commission said offense, including but not limited to a sum of money in United States currency representing the amount of proceeds traceable to the commission of said offense.

Substitute Assets Provision

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

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third person;
- c. has been placed beyond the jurisdiction of the Court;


d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be subdivided without difficulty;

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

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


FOREPERSON


GEOFFREY S. BERMAN
United States Attorney

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

ZHU HUA,
a/k/a "Afwar,"
a/k/a "CVNX,"
a/k/a "Alayos,"
a/k/a "Godkiller," and
ZHANG SHILONG,
a/k/a "Baobeilong,"
a/k/a "Zhang Jianguo",
a/k/a "Atreexp,"

Defendants.

SEALED INDICTMENT

18 Cr. ____

(18 U.S.C. §§ 1030(b), 1349,
1028A(a)(1) & (b), and 2.)

GEOFFREY S. BERMAN

United States Attorney.

TRUE BILL 


FOREPERSON
