

FILED

MAY 07 2019

U.S. DISTRICT COURT
INDIANAPOLIS, INDIANA

SEALED

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF INDIANA
INDIANAPOLIS DIVISION

UNITED STATES OF AMERICA,)
)
 Plaintiff,)
)
 v.)
)
 FUJIE WANG,)
 a/k/a "Dennis Wang,")
 JOHN DOE,)
 a/k/a "Deniel Jack,")
 a/k/a "Kim Young,")
 a/k/a "Zhou Zhihong,")
)
 Defendants.)

Cause No. _____

18 U.S.C. § 371
18 U.S.C. § 1349
18 U.S.C. § 1030(a)(5)(A)

1 : 19 - cr - 153 ^{JRS} -MJD

INDICTMENT

The Grand Jury charges that:

BACKGROUND

At all times relevant to all counts of this Indictment:

Defendants

1. Defendant FUJIE WANG, a/k/a "Dennis Wang" ("WANG"), was a national of the People's Republic of China ("China"), and a resident of Shenzhen, China. When set forth in the Chinese convention with the surname coming first, his name was Wang Fujie (王福杰 in Chinese Hanzi). He used the Western nickname "Dennis."

2. The true name of defendant JOHN DOE, a/k/a "Zhou Zhihong," a/k/a "Kim Young," a/k/a "Deniel Jack," is not known to the Grand Jury. He used the names "Deniel Jack," "Kim Young," and "Zhou Zhihong," as well as various online nicknames. His activities were based in China.

3. Defendants WANG and DOE (hereinafter “Defendants”) and others known and unknown to the Grand Jury were members of an extremely sophisticated hacking group operating in China and targeting large businesses in the United States, including in the Southern District of Indiana and elsewhere.

Victim Entities

4. Anthem, Inc. (“Anthem”), headquartered in Indianapolis in the Southern District of Indiana, was one of the largest health benefits companies in the United States. Many of the health benefits services Anthem provided, including insurance coverage to individuals, are well known to the general public. To provide insurance to its customers, Anthem had to store and use large amounts of customer data, including personally identifiable information and confidential business information, in its computer networks.

5. Victim Business 1 was a large U.S.-based business in the technology sector.

6. Victim Business 2 was a large U.S.-based business in the basic materials sector.

7. Victim Business 3 was a large U.S.-based business in the communication services sector.

8. Victim Businesses 1, 2 and 3 all had to store and use large amounts of data, including confidential business information, on their computer networks.

Other Businesses

9. Alipay was a third-party mobile and online payment platform. Ant Financial Services Group, headquartered in China, operated Alipay.

10. Citrix ShareFile was an Internet-based data storage and transfer service. Citrix ShareFile was a wholly owned subsidiary of Citrix Systems, Inc. A unique user account was required for an individual to access and utilize the Citrix ShareFile service. At the time of the

events described in this Indictment, a user could create a Citrix ShareFile account, which was associated with a specific domain, on a trial basis without providing payment information. Further, although users were asked to provide a registration email address, Citrix ShareFile did not employ any security measures such as email authentication to determine whether the email address provided was actually real or valid. Anthem did not own or have an established relationship with Citrix ShareFile and had not authorized any individual to share Anthem information with the Citrix ShareFile service.

Definitions

11. The following definitions explain the terms used in this Indictment:
 - a. “Domain” was short for “domain name.” Under 18 U.S.C. § 3559(g)(2)(B), the definition of “domain name” is based on the Trademark Act, under 15 U.S.C. § 1127. Under the Trademark Act, “domain name” means “any alphanumeric designation which is registered with or assigned by any domain name registrar, domain name registry, or other domain name registration authority as part of an electronic address on the Internet.” A “subdomain” was a subdivision of a domain.
 - b. The Domain Name System (“DNS”) was a hierarchical and decentralized Internet service that translated domain names into Internet Protocol (“IP”) addresses. A “top-level domain” was the last segment (i.e., suffix) in a domain (e.g., “.com” or “.net”), associated with the highest level of the DNS.
 - c. A “driver” was software, provided by a hardware maker, which told the computer’s operating system exactly how to work with that hardware.

- d. “Harvesting” was the practice of stealing legitimate user credentials to gain access to computer systems for malicious purposes.
- e. “Hosting” was a service through which storage and computing resources are provided to a customer. A provider that provided hosting could be called a “host” or a “hosting provider.”
- f. “Malware” was malicious software. Once a system was compromised by malware, a malicious actor could install a “backdoor” tool, which would provide the actor with remote access to the compromised computer. Malicious actors could encode domains or subdomains into the backdoor, and then point them to an actor-controlled server (known as a “command and control server”) that would then control the compromised computer.
- g. “Pointing” a domain or subdomain was an action to associate it with a specific IP address in DNS records.
- h. “Registration” was the act of reserving a domain on the Internet for a specific time period. In order to do so, the domain registrant would usually apply online to a company that managed the reservation of Internet domain names, known as a registrar. A registrar operated in accordance with the guidelines of the designated organizations that managed top-level domains, known as registries. The domain name registrant was bound by the terms and conditions of the registrar with which it registered its domain name, for instance adhering to a certain code of conduct or indemnifying the registrar and registry against any legal or civil action taken as a result of use of the domain name.

- i. A “server” was a type of computer or device on a network that managed network resources.
- j. “Spearfishing” was an electronic mail (“email”) or electronic communications scam targeted towards a specific individual, organization, or business.
- k. “Validation” was the process by which domain registrars ensure that accurate and valid registration details are associated with domains. Legitimate domain registrars were required to validate the registration information associated with a domain, starting in 2013. Registrars typically sent an email to a registrant requiring an affirmative response through a tool-based authentication method. Under this method of validation, the registrant of the domain must have had control of the email account associated with the domain in order to receive and respond to the validation request sent to the account.
- l. A “virtual private server,” or VPS, was a virtual server that a user perceived as a single physical server, even though it was installed on a physical server potentially running multiple operating systems.

The Hacking Group

12. From on or about February 18, 2014, to on or about January 31, 2015, members of a hacking group operating in China and including Defendants, conducted campaigns of intrusions into U.S.-based computer systems. They gained entry to the computer systems of Anthem, Victim Business 1, Victim Business 2, and Victim Business 3 (hereinafter the “Victims”). As part of this international computer hacking scheme, Defendants:

- a. Used spearfishing, malware, and other sophisticated techniques to hack into the computer networks of the Victims without authorization;
- b. Installed malware and tools to the compromised computer systems to further compromise the computer networks of the Victims;
- c. Identified data of interest on the compromised computers, including personally identifiable information and confidential business information; and
- d. Collected files and other information from the compromised computers and then stole (i.e., exfiltrated) this data of interest using encrypted archives and computers under their control.

COUNT ONE

(Conspiracy to Commit Fraud and Related Activity in Connection with Computers)

18 U.S.C. § 371

13. Beginning at least on or about February 18, 2014, and continuing until at least on or about January 31, 2015, in the Southern District of Indiana and elsewhere, defendants FUJIE WANG, a/k/a “Dennis Wang,” and JOHN DOE, a/k/a “Deniel Jack,” a/k/a “Kim Young,” a/k/a “Zhou Zhihong,” and others known and unknown to the Grand Jury, did knowingly and intentionally conspire and agree to commit offenses against the United States, that is:

- a. to intentionally access a computer without authorization, and exceed authorized access, and thereby obtain information from a protected computer, and the value of the information obtained exceeded \$5,000, all in violation of Title 18, United States Code, Sections 1030(a)(2), and (c)(2)(B)(iii);

- b. to knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally cause damage without authorization to a protected computer, and cause loss to persons during a 1-year period from Defendants' course of conduct affecting protected computers aggregating at least \$5,000 in value, and cause damage affecting 10 or more protected computers during a 1-year period, all in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B); and,
- c. to knowingly transfer and possess and use, in or affecting interstate or foreign commerce, without lawful authority, a means of identification of another person, to wit, names, Social Security numbers, and dates of birth, with the intent to commit, and in connection with, any unlawful activity that constitutes a violation of Federal law, to wit, violations of Section 1030 of Title 18 of the United States Code, in violation of Title 18, United States Code, Sections 1028(a)(7), (b)(2)(B), and (f).

Manner and Means of the Conspiracy

- 14. It was part of the conspiracy that:
 - a. Defendants used extremely sophisticated techniques to hack into the computer networks of the Victims. These techniques included the sending of specially-tailored spearfishing emails with embedded hyperlinks to employees of the Victims. After a user accessed the hyperlink, a file was downloaded which, when executed, deployed malware that would compromise the user's computer system by, in pertinent part, installing a

backdoor enabling remote access to that computer system through a command and control server controlled by Defendants.

- b. After Defendants had obtained the ability to remotely access a computer system on a Victim's network, they then sought to move laterally across the Victim's computer network and escalate their privileges on the network (i.e., gain increasingly greater ability to access information and make changes in the Victim's network environment). Defendants sometimes patiently waited months before taking further action, quietly maintaining access to the Victim's network.
- c. After Defendants had sufficient access to the Victim's network, they engaged in reconnaissance by searching the network for data of interest. This data included personally identifiable information and confidential business information. For example, Defendants identified and ultimately stole data concerning approximately 78.8 million persons from Anthem's computer network, including names, health identification numbers, dates of birth, Social Security numbers, addresses, telephone numbers, email addresses, employment information, and income data.
- d. Once the data of interest had been identified and located, Defendants then collected the relevant files and other information from the compromised computers using software tools.
- e. After the data of interest had been collected, Defendants stole the data of interest by placing it into encrypted archive files and then sending it through multiple computers to destinations in China. They did this, in

pertinent part, by using the Citrix ShareFile data storage and transfer service.

- f. Defendants then deleted the encrypted archive files that they had previously created, in an attempt to avoid detection.

15. It was further part of the conspiracy that Defendants knowingly falsely registered a domain and knowingly used that domain in the course of the offense, in violation of 18 U.S.C. § 3559(g)(1).

Overt Acts

16. In furtherance of the conspiracy and to effect its unlawful object, Defendants committed and caused to be committed the following overt acts in the Southern District of Indiana and elsewhere:

- a. On or about February 18, 2014, Defendants transmitted a spearfishing email to employees of an Anthem subsidiary, resulting in the execution of malware on at least one of the subsidiary's computers.
- b. On or about May 13, 2014, Defendants accessed the computer network of Anthem, then accessed an Anthem computer located in the Southern District of Indiana, then caused the transmission of a program, information, code, and command on that computer, all without authorization.
- c. On or about July 8, 2014, defendant WANG validated with the applicable registrar his control over a domain (hereinafter "Domain 1") he had previously registered using false information.

- d. In or about September 2014, Defendants accessed the computer network of Victim Business 1 and utilized malware associated with a backdoor encoded with a subdomain of Domain 1, all without authorization.
- e. In or about October 2014 and November 2014, on multiple occasions, Defendants accessed the computer network of Anthem without authorization for the purpose of conducting reconnaissance on Anthem's enterprise data warehouse, a system that stores a large amount of personally identifiable information.
- f. On or about October 28, 2014, defendant DOE used an Alipay account to pay for the use of a VPS located in the state of Arizona (hereinafter "Arizona VPS").
- g. On or about October 29, 2014, defendant DOE accessed the computer network of Anthem and then, using the Arizona VPS and the Citrix ShareFile service, transferred a software tool designed to harvest user credentials to an Anthem computer, all without authorization.
- h. On or about October 29, 2014, defendant DOE accessed the computer network of Anthem and then, using the Citrix ShareFile service, transferred an archive file containing harvested Anthem user credentials to a computer he controlled, all without authorization.
- i. In or about November 2014, Defendants accessed the computer network of Victim Business 2 and then, using the Citrix ShareFile service, stole archive files containing confidential business information, all without authorization.

- j. On or about November 9, 2014, Defendants accessed the computer network of Anthem, then accessed an Anthem computer located in the Southern District of Indiana, then caused the transmission of a program, information, code, and command on that computer, all without authorization.
- k. On or about November 12, 2014, Defendants accessed the computer network of Anthem and then accessed Anthem's enterprise data warehouse, all without authorization.
- l. In or about December 2014 and January 2015, on multiple occasions, Defendants accessed the computer network of Anthem, accessed Anthem's enterprise data warehouse, queried the enterprise data warehouse for personally identifiable information, and compressed and encrypted the resulting output into archive files, all without authorization.
- m. On or about December 8, 2014, defendant DOE accessed the computer network of Anthem and then transferred a software tool to an Anthem computer, all without authorization.
- n. On or about December 17, 2014, defendant WANG prospectively pointed four subdomains of another domain (hereinafter "Domain 2") to an IP address that Defendants intended to associate with a VPS located in the state of California (hereinafter the "California VPS").
- o. On or about December 17, 2014, Defendants created the California VPS, which was paid for using Alipay, causing the four subdomains of Domain 2 previously pointed by defendant WANG to be associated with the VPS.

- p. On or about December 17, 2014, defendant WANG registered Domain 2 with the applicable registrar, using false information.
- q. In or about January 2015, on multiple occasions, Defendants accessed the computer network of Anthem, accessed Anthem's enterprise data warehouse, and transferred encrypted archive files containing personally identifiable information from Anthem's enterprise data warehouse to computers they controlled in the United States using the Citrix ShareFile service, all without authorization.
- r. In or about January 2015, on multiple occasions, Defendants transferred encrypted archive files containing personally identifiable information from Anthem's enterprise data warehouse from computers they controlled in the United States to computers they controlled in China.
- s. In or about January 2015, Defendants accessed the computer network of Victim Business 3 without authorization.
- t. On or about January 8, 2015, Defendants, using the California VPS, created an email account later used to send spearfishing emails to employees of Victim Business 3.
- u. On or about January 9, 2015, Defendants transmitted spearfishing emails to employees of Victim Business 3.
- v. On or about January 12, 2015, Defendants transmitted spearfishing emails to employees of Victim Business 3.
- w. On or about January 27, 2015, using a computer they controlled in the United States, Defendants deleted from the Citrix ShareFile service certain

archive files containing personally identifiable information that they had previously transferred there from Anthem's enterprise data warehouse, all without authorization.

- x. On or about January 28, 2015, using a computer they controlled in the United States, Defendants deleted from the Citrix ShareFile service certain archive files containing personally identifiable information that they had previously transferred there from Anthem's enterprise data warehouse, all without authorization.
- y. On or about January 31, 2015, Defendants' access to the computer network of Anthem was terminated due to the implementation of incident response measures by Anthem.

All of which is a violation of Title 18, United States Code, Section 371.

COUNT TWO

(Conspiracy to Commit Wire Fraud)

18 U.S.C. § 1349

18. The allegations contained in paragraphs 14 through 16 of Count One of this Indictment are re-alleged and incorporated as though fully set forth in this paragraph.

19. Beginning at least on or about February 18, 2014, and continuing until at least on or about January 31, 2015, in the Southern District of Indiana and elsewhere, defendants FUJIE WANG, a/k/a "Dennis Wang," and JOHN DOE, a/k/a "Deniel Jack," a/k/a "Kim Young," a/k/a "Zhou Zhihong," did knowingly and intentionally conspire and agree 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, and to transmit and cause to be transmitted by means of

wire communications in interstate and foreign commerce certain writings, signs, signals, and sounds in furtherance of such scheme and artifice, contrary to Title 18, United States Code, Section 1343.

All of which is a violation of Title 18, United States Code, Section 1349.

COUNTS THREE and FOUR

(Intentional Damage to a Protected Computer)

18 U.S.C. §§ 1030(a)(5)(A) and (c)(4)(B)

20. The allegations contained in paragraphs 14 through 16 of Count One of this Indictment are re-alleged and incorporated as though fully set forth in this paragraph.

21. On or about each of the dates set forth below in each separate count, in the Southern District of Indiana and elsewhere, defendants FUJIE WANG, a/k/a “Dennis Wang,” and JOHN DOE, a/k/a “Deniel Jack,” a/k/a “Kim Young,” a/k/a “Zhou Zhihong,” knowingly caused the transmission of a program, information, code, and command and, as a result of such conduct, intentionally caused damage without authorization to a protected computer, and the offense caused loss to persons during a 1-year period from Defendants’ course of conduct affecting protected computers aggregating at least \$5,000 in value, and caused damage affecting 10 or more protected computers during a 1-year period, described below for each count, each transmission constituting a separate count:

COUNT			
3	May 13, 2014	Anthem, Inc.	Indianapolis
4	November 9, 2014	Anthem, Inc.	Indianapolis

Each Count of which is a separate violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B), and 2.

FORFEITURE ALLEGATION AS TO COUNT TWO

22. As a result of committing the offenses charged in Count 2 of this Indictment, defendants FUJIE WANG, a/k/a “Dennis Wang,” and JOHN DOE, a/k/a “Deniel Jack,” a/k/a “Kim Young,” a/k/a “Zhou Zhihong,” shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(D)(vi) and Title 28, United States Code, Section 2461, all property, real and personal, that constitutes or is derived from proceeds traceable to the commission of the said offense, and all property traceable thereto.

FORFEITURE ALLEGATION AS TO COUNTS THREE AND FOUR

23. As a result of committing the offenses charged in Counts Three and Four of this Indictment, defendants FUJIE WANG, a/k/a “Dennis Wang,” and JOHN DOE, a/k/a “Deniel Jack,” a/k/a “Kim Young,” a/k/a “Zhou Zhihong,” shall forfeit to the United States:

- a. pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i), any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly as a result of the offenses charged in Counts One, Three, and Four of this Indictment; and
- b. pursuant to Title 18, United States Code, Section 1030(i), all right, title, and interest in any personal property that was used or intended to be used to commit or to facilitate the commission of the offenses charged in Counts One, Three, and Four of this Indictment.

SUBSTITUTE ASSETS PROVISION

(Applicable to All Forfeiture Allegations)

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

- 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 which cannot be divided without difficulty;

//

//

//

//

//

//

//

//

//

//

//

//

//

the United States shall be entitled, pursuant to 21 U.S.C. § 853(p) (as incorporated by 28 U.S.C. § 2461(c) and 18 U.S.C. §§ 982(b) and 1030(i)), to forfeiture of any other property of the defendants up to the value of the above-described forfeitable property.

A TRUE BILL:



FOREPERSON

JOSH MINKLER
UNITED STATES ATTORNEY

BRIAN A. BENCZKOWSKI
ASSISTANT ATTORNEY GENERAL



Steven D. DeBrot
Assistant United States Attorney



William A. Hall, Jr.
Senior Counsel
Criminal Division, Computer Crime and Intellectual Property Section