2019R00508/APT/VSL

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	Hon.
	:	
v.	:	Crim. No. 24-
	:	
TA VAN TAI,	:	18 U.S.C. § 371
a/k/a "Quynh Hoa,"	:	18 U.S.C. § 1349
a/k/a "Bich Thuy,"	:	18 U.S.C. § 1030(a)(4)
NGUYEN VIET QUOC,	:	18 U.S.C. § 1028A(a)(1)
a/k/a "Tien Nguyen,"	:	18 U.S.C. § 1028(f)
NGUYEN TRANG XUYEN, and	:	18 U.S.C. § 1956(h)
NGUYEN VAN TRUONG,	:	18 U.S.C. § 2
a/k/a "Chung Nguyen"	:	

INDICTMENT

The Grand Jury in and for the District of New Jersey, sitting at Newark, charges as follows:

COUNT 1
(Conspiracy to Commit Fraud and Related Activity in Connection with Computers)

Overview

1. From at least as early as in or around May 2018 through at least as late as in or around October 2021, defendants TA VAN TAI, a/k/a "Quynh Hoa," a/k/a "Bich Thuy" ("TAI"), NGUYEN VIET QUOC, a/k/a "Tien Nguyen" ("QUOC"), NGUYEN TRANG XUYEN ("XUYEN"), NGUYEN VAN TRUONG, a/k/a "Chung Nguyen" ("TRUONG"), and others were part of a financially motivated cybercriminal conspiracy known as "FIN9". Through the conspiracy, the Defendants and others accessed the computer networks of companies throughout the United States (the "Victim Companies") without authorization and used that access to steal or attempt

to steal non-public information, employee benefits, and funds (the "Network Intrusions"). Through the Network Intrusions, the Defendants caused losses to the Victim Companies in excess of $71 million.

Relevant Individuals and Entities

2. At all times relevant to this Indictment:

a. TAI, QUOC, XUYEN, and TRUONG were citizens of, and resided in, the Socialist Republic of Vietnam.

b. Company-1 was a cloud hosting company headquartered in West Palm Beach, Florida.

c. Company-2 was a cloud storage and file synchronization service provider headquartered in San Francisco, California.

d. Company-3 was a peer-to-peer cryptocurrency platform headquartered in Wilmington, Delaware.

e. Company-4 was a package forwarding service provider headquartered in Portland, Oregon.

f. Company-5 was a video game, consumer electronics, and gaming merchandise retailer headquartered in Grapevine, Texas.

g. Company-6 was cloud-based software development platform with headquarters in San Francisco, California.

h. Application-1 was a voice over IP ("VoIP") and instant messaging software application.

i. Cardholder Victim-1 resided in Anaheim, California.

j. Victim-1 was an electronics company with its North American headquarters in Newark, New Jersey.

k. Victim-2 was a global provider of technology products and services headquartered in Centennial, Colorado.

l. Victim-3 was a nonprofit organization headquartered in Los Angeles, California.

m. Victim-4 was a fashion company with offices in New York, New York.

Relevant Terms

n. "Phishing" is the fraudulent practice of sending emails or other electronic communications purporting to be from a reputable or known source in order to induce the individual or individuals receiving the communications to reveal personal information, such as account login information, passwords, and credit card information.

o. "Spear Phishing" is the act of sending emails to specific and well-researched targets while purporting to be a trusted sender. The aim of a spear phishing campaign is often to obtain unauthorized access to the victim's computer network.

p. "Malicious code" or "malicious computer scripts" refer to harmful computer code or files designed to create or exploit vulnerabilities within a computer network.

q. A "supply chain attack" is a type of cyberattack that seeks to damage an organization by targeting the computer networks of trusted third-party vendors who offer services or software vital to the supply chain.

Goal of the Conspiracy

3. The goal of the conspiracy was for TAI, QUOC, XUYEN, TRUONG, and others to enrich themselves by fraudulently obtaining access to the Victim Companies through the Network Intrusions, and using that access to steal non-public information, employee benefits, and funds.

Manner and Means of the Conspiracy

4. It was part of the conspiracy that:

a. The Co-Conspirators obtained unauthorized access to the computer networks of the Victim Companies through phishing campaigns or other methods, such as supply chain attacks, designed to provide the Co-Conspirator's with control over the Victim Companies' networks.

b. After gaining access to the Victim Companies' networks, the Co-Conspirators used that access to exfiltrate or attempt to exfiltrate non-public information, employee benefits, and/or funds. For example, the Co-Conspirators accessed employee benefit rewards programs maintained by the Victim Companies and re-directed digital employee benefits (most prominently, gift cards) to accounts controlled by Defendants. The Co-Conspirators also stole gift card information stored on the computer networks of certain Victim Companies.

c. The Co-Conspirators compromised electronic payment systems at financial institutions in the United States and abroad that were used by the Victim Companies to process financial transactions.

d. The Co-Conspirators stole personally identifiable information and credit card information associated with employees and customers of the Victim Companies. In an effort to obfuscate their own identities and evade detection by law enforcement, the Co-Conspirators would, at times, use that information in furtherance of the conspiracy by, for example, registering online accounts at cryptocurrency exchanges or server hosting companies in the names of individuals whose identities were stolen.

e. The Co-Conspirators used accounts and servers held at Company-1 to: (a) access the computer networks of Victim Companies; and (b) exfiltrate and store data obtained through the Network Intrusions. For example, the Co-Conspirators accessed Victim-1's network through a server ("Server-1") that was assigned to an account ("Account-1") held at Company-1.

f. The Co-Conspirators additionally used accounts held at Company-2 to exfiltrate and store Victim Company data stolen through the Network Intrusions.

g. The Co-Conspirators used personal devices to act as two-factor authorization devices to access and maintain access to certain Victim Company networks, including the network of Victim Company-2.

h. To monetize the Network Intrusions, the Co-Conspirators sold stolen gift cards to individuals in exchange for cryptocurrency, most commonly

Bitcoin, through social media accounts and peer-to-peer cryptocurrency exchanges, such as Company-3.

i. The Co-Conspirators used Google searches to (a) conduct research on the Victim Companies; (b) look up financial transactions related to the Network Intrusions; and (c) search for information regarding law enforcement investigations that could reveal the Co-Conspirators.

j. The Co-Conspirators used Application-1 to discuss the monetization of gift cards obtained through the Network Intrusions.

k. TAI directed TRUONG to send the proceeds from the sale of stolen gift cards to specific accounts.

l. The Co-Conspirators used stolen gift card proceeds to pay for services used in connection with the Network Intrusions and the monetization of stolen gift cards, including server and web domain hosting services.

m. The Co-Conspirators used accounts held at Company-6 to store malicious computer scripts used by the Co-Conspirators to facilitate the Network Intrusions.

Overt Acts

5. In furtherance of the conspiracy, and to effect its objects, Defendants and others committed the following overt acts, among others, in the District of New Jersey, and elsewhere:

a. In or around May 2019, the Co-Conspirators accessed, without authorization, Victim-1's Employee Recognition and Rewards Benefits System ("ERRBS"), using stolen login credentials (the "Victim-1 Intrusion"). The ERRBS

enabled Victim-1 employees to accrue points and rewards that could be redeemed for gift cards issued by various retail merchants. The Co-Conspirators used the access to Victim-1's ERRBS to issue approximately 7,617 gift cards—worth approximately $1 million—to email accounts under their control, including gift cards issued by Company-5.

b. In or around May 2019, during the Victim-1 Intrusion, QUOC accessed Server-1, which contained evidence of the Victim-1 Intrusion, such as usernames and passwords of Victim-1's employees.

c. On or about May 13, 2019, during the Victim-1 Intrusion, XUYEN conducted a Google search for "Fin9 group".

d. From on or about May 9, 2019 through on or about May 12, 2019, using Application-1, TAI sent TRUONG information for dozens of gift cards that were stolen from Victim-1. For example, on or about May 12, 2019, TAI sent TRUONG a message that said, in sum and substance when translated to English, "Here's 1000 of [Company-5], hold on to them to sell." In the following message, TAI sent TRUONG a list of ten gift card numbers and a corresponding PIN number for each card.

e. From in or around May 2019 through in or around June 2019, the Co-Conspirators, through a server assigned to Account-1, accessed, without authorization, Victim-2's computer network (the "Victim-2 Intrusion").

f. On or about May 24, 2019, QUOC used his iPhone as a two-factor authentication method so that the Co-Conspirators could maintain their access to Victim-2's network.

g. Between on or about February 9, 2019 and on or about April 14, 2019, TAI and QUOC accessed Account-1, which contained evidence of the Victim-2 Intrusion, including unauthorized connections to Victim-2's network, usernames and passwords for accounts on Victim-2's network, and documents with Victim-2's customers' information.

h. Between on or about March 14, 2019 and on or about March 19, 2019, the Co-Conspirators stole approximately $50,000 worth of gift cards from Victim-4.

i. On or about March 20, 2019, XUYEN conducted a Google search for "sell [Victim-4] gift card to bitcoin."

j. On or about March 21, 2019, XUYEN conducted a Google search for "how many giftcard [Victim-4] using per order."

k. On or about March 22, 2019, XUYEN conducted a Google search for "Victim-4 breach."

l. On or about April 17, 2019, using Application-1, in response to a question from TRUONG about whether TAI had "any other gifts," TAI responded that he had "just [Victim-4], that's all." TRUONG responded to TAI that he would take the Victim-4 gift cards.

m. Between on or about May 11, 2019 and on or about May 14, 2019, TRUONG sold gift cards stolen from the Victim Companies to others online, including on social media platforms and peer-to-peer cryptocurrency marketplaces such as Company-3.

n. On or about April 26, 2019, TAI sent TRUONG messages on an online platform that said, in sum and substance when translated to English, "100k into this account please, send it for me." In a subsequent message, TAI sent TRUONG information for a bank account held at a Vietnamese bank.

o. In or around September 2016, TAI registered an account at Company-2 that was used to store data stolen from Victim Companies.

p. In or around May 2019, QUOC accessed Server-1, which was used in connection with the Victim-1 and Victim-2 Intrusions.

q. In or around February 2021, XUYEN accessed a server hosted by Company-1 during the same time period it was used to compromise Victim-3.

All in violation of Title 18, United States Code, Section 371.

COUNT 2
(Conspiracy to Commit Wire Fraud)

1. The allegations in paragraphs 2 through 5 of Count 1 of this Indictment are re-alleged and incorporated as though fully set forth in this paragraph.

2. From at least as early as in or around May 2018 through at least as late as in or around October 2021, in the District of New Jersey and elsewhere, the defendants,

TA VAN TAI,
a/k/a "Quynh Hoa,"
a/k/a "Bich Thuy,"
NGUYEN VIET QUOC,
a/k/a "Tien Nguyen,"
NGUYEN TRANG XUYEN, and
NGUYEN VAN TRUONG,
a/k/a "Chang Nguyen,"

did knowingly and intentionally conspire with others to devise, and intend 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, for the purpose of executing and attempting to execute such scheme and artifice to defraud, did transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, to wit, a wire transmission sent on or about May 30, 2019, from a location outside of New Jersey to a location inside of New Jersey, contrary to Title 18, United States Code, Section 1343.

In violation of Title 18, United States Code, Section 1349.

COUNTS 3 AND 4
(Computer Fraud and Abuse)

1. The allegations in paragraphs 2 through 5 of Count 1of this Indictment are re-alleged and incorporated as though fully set forth in this paragraph.

2. In or around May 2019, in the District of New Jersey, and elsewhere, the defendants,

TA VAN TAI,
a/k/a "Quynh Hoa,"
a/k/a "Bich Thuy,"
NGUYEN VIET QUOC,
a/k/a "Tien Nguyen,"
NGUYEN TRANG XUYEN, and
NGUYEN VAN TRUONG,
a/k/a "Chang Nguyen,"

did, knowingly and with intent to defraud, access a protected computer without authorization, and by means of such conduct further the intended fraud and obtain anything of value; to wit, Defendants, without authorization, accessed the computer networks of the Victim Companies set forth more fully below, and used that access to steal non-public information, employee benefits, and funds, each such instance constituting a separate count of this Indictment:

Count	Date(s)	Description
Count 3	In or around May 2019	Access to the computer network of Victim-1.
Count 4	From in or around May 2019 through in or around June 2019	Access to the computer network of Victim-2.

In violation of Title 18, United States Code, Section 1030(a)(4) and Section 2.

COUNT 5
(Aggravated Identity Theft)

1. The allegations in paragraphs 2 through 5 of Count 1 of this Indictment are re-alleged and incorporated as though fully set forth in this paragraph.

2. From in or around February 2019 through in or around September 2019, in the District of New Jersey, and elsewhere, the defendants,

TA VAN TAI,
a/k/a "Quynh Hoa,"
a/k/a "Bich Thuy," and
NGUYEN VIET QUOC,

did knowingly use, without lawful authority, a means of identification of another person, namely a credit card bearing the name and account number of Cardholder Victim-1, during and in relation to a felony violation enumerated in Title 18, United States Code, Section 1028A, that is, conspiracy to commit wire fraud in violation of Title 18, United States Code, Section 1349 as charged in Count 2, knowing that the means of identification belonged to another actual person.

In violation of Title 18, United States Code, Section 1028A(a)(1) and Section 2.

COUNT 6

(Conspiracy to Commit Fraud in Connection with Identification Documents)

1. The allegations in paragraphs 2 through 5 of Count 1 of this Indictment are re-alleged and incorporated as though fully set forth in this paragraph.

2. From in or around February 2019 through in or around September 2019, in the District of New Jersey, and elsewhere, the defendants,

TA VAN TAI,
a/k/a "Quynh Hoa,"
a/k/a "Bich Thuy," and
NGUYEN VIET QUOC,

did knowingly and intentionally conspire and agree with each other and others to use in or affecting interstate or foreign commerce, without lawful authority, a means of identification of another person, knowing that the means of identification belonged to another actual person, in connection with a violation of Federal law, namely, wire fraud, and as a result of the offense, defendants TAI and NGUYEN obtained anything of value aggregating $1,000 or more from in or around February 2019 through in or around September 2019, contrary to Title 18, United States Code, Section 1028(a)(7).

In violation of Title 18, United States Code, Section 1028(f) and Section 1028(b)(1)(D).

COUNT 7
(Conspiracy to Commit Money Laundering)

1. The allegations in paragraphs 2 through 5 of Count 1 of this Indictment are re-alleged and incorporated as though fully set forth in this paragraph.

Overview

2. From in or around May 2018 through in or around October 2021, in the District of New Jersey, and elsewhere, the defendants,

TA VAN TAI,
a/k/a "Quynh Hoa,"
a/k/a "Bich Thuy,"
NGUYEN TRANG XUYEN, and
NGUYEN VAN TRUONG,
a/k/a "Chang Nguyen,"

did knowingly and intentionally conspire and agree with each other and others to knowingly conduct and attempt to conduct financial transactions affecting interstate and foreign commerce, which transactions involved the proceeds of specified unlawful activity, namely, wire fraud, in violation of Title 18, United States Code, Section 1343 and computer fraud and abuse, in violation of Title 18, United States Code, Section 1030(a)(4), knowing that the transactions were designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, knowing that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, contrary to Title 18, United States Code, Section 1956(a)(1)(B)(i).

Goal of the Conspiracy

3. The goal of the conspiracy was for TAI, XUYEN, TRUONG, and others to conduct financial transactions involving money obtained from the Victim Companies alleged in this Indictment, in order to conceal and disguise the nature, location, source, ownership, and control of the money.

Manner and Means of the Conspiracy

4. It was part of the conspiracy that:

a. TAI stole gift cards from the Victim Companies and provided the gift cards to TRUONG, who monetized them. For example, between on or about May 11, 2019 and on or about May 13, 2019, TAI sent TRUONG messages on Application-1 with information for 56 gift cards stolen from Victim-1.

b. The Co-Conspirators used an account at Company-3 ("Account-2") to sell approximately 1,756 gift cards that were stolen from Victim-1. For example, on or about the same date the Co-Conspirators first compromised Victim-1's systems, a user of Account-2 sold gift cards stolen from Victim-1 and asked a purchaser, "Do you want more?" The user of Account-2 explained, "I have in bulk."

c. TRUONG sold the gift cards to third parties, including on social media platforms and peer-to-peer cryptocurrency marketplaces.

d. On or about April 17, 2019, TAI told TRUONG, via Application-1, that TRUONG had to tell the individuals to whom he sold the gift cards to "use a fake IP" address. TRUONG explained that, "[e]ven with dirty gift cards, [his customers] are still game, as long [as the gift cards] passed at the time of the order."

e. XUYEN used an account at Company-3 ("Account-3") for the

purpose of receiving cryptocurrency from the sale of stolen gift cards. On or about the same date Company-3 requested Account-3 to provide documents to verify the account, TAI messaged XUYEN with the name of the individual listed for Account-3. XUYEN responded with a link to an online domain that offers fake identification documents for sale.

In violation of Title 18, United States Code, Section 1956(h).

FORFEITURE ALLEGATION AS TO COUNTS 1, 3, AND 4

1. As a result of committing the offenses charged in Counts 1, 3, and 4 of this Indictment, the defendants charged in each such count 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 1, 3, and 4 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 1, 3, and 4 of this Indictment.

FORFEITURE ALLEGATION AS TO COUNT 2

2. As a result of committing the wire fraud offense constituting specified unlawful activity as defined in Title 18, United States Code, Section 1956(c)(7), as alleged in Count 2 of this Indictment, the defendants charged in that count, 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), all property, real and personal, that constitutes or is derived from proceeds traceable to the commission of the offense charged in Count 2, and all property traceable thereto.

FORFEITURE ALLEGATION AS TO COUNT 6

3. As a result of committing the offense in violation of Title 18, United States Code, Section 1028 alleged in Count 6 of this Indictment, the defendants charged in that count shall forfeit to the United States:

a. pursuant to Title 18, United States Code, Section 982(a)(2)(B), any property constituting, or derived from, proceeds obtained directly or indirectly, as a result of such offense; and

b. pursuant to Title 18, United States Code, Section 1028(h), any and all illicit authentication features, identification documents, document-making implements and means of identification.

FORFEITURE ALLEGATION AS TO COUNT 7

4. As a result of committing the money laundering offense charged in Count 7 of this Indictment, the defendants charged in that count shall forfeit to the United States, pursuant to Title 18, United States Code, Section 982(a)(1), all property, real or personal, involved in such money laundering offenses, and all property traceable to such property.

Substitute Assets Provision
(Applicable to All Forfeiture Allegations)

5. 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), as incorporated by Title 28, United States Code, Section 2461(c), to seek forfeiture of any other property of the defendant up to the value of the above-described forfeitable property.

A TRUE BILL

[redacted]

FOREPERSON

Philip R. Sellinger

PHILIP R. SELLINGER
United States Attorney

CASE NUMBER: 24-

United States District Court
District of New Jersey

UNITED STATES OF AMERICA
v.
TA VAN TAI,
a/k/a "Quynh Hoa,"
a/k/a "Bich Thuy,"
NGUYEN VIET QUOC,
a/k/a "Tien Nguyen,"
NGUYEN TRANG XUYEN, and
NGUYEN VAN TRUONG,
a/k/a "Chang Nguyen"

INDICTMENT FOR
18 U.S.C. § 371
18 U.S.C. § 1349
18 U.S.C. § 1030(a)(4)
18 U.S.C. § 1028A(a)(1)
18 U.S.C. § 1028(f)
18 U.S.C. § 1956(h)
18 U.S.C. § 2

A True Bill,
[redacted]
Foreperson

PHILIP R. SELLINGER
UNITED STATES ATTORNEY
FOR THE DISTRICT OF NEW JERSEY

ANTHONY P. TORNTORE
VINAY S. LIMBACHIA
ASSISTANT U.S. ATTORNEYS
NEWARK, NEW JERSEY
973-353-6071