U.S. Department of
JUSTICE

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

UNITED STATES OF AMERICA

v.

XU ZEWEI (徐泽伟), and

ZHANG YU (张宇),

Defendants.

Criminal No. **4:23-cr-00523**

Filed Under Seal

INDICTMENT

THE UNITED STATES GRAND JURY CHARGES:

INTRODUCTION

At all times relevant to this Indictment:

1. The Shanghai State Security Bureau ("SSSB") was a foreign intelligence arm of the People's Republic of China's ("PRC") Ministry of State Security ("MSS"), headquartered in Shanghai, China. The MSS and the SSSB had responsibility for the PRC's domestic counter-intelligence, non-military foreign intelligence, and aspects of the PRC's political and domestic security.

2. From February 2020 to June 2021, SSSB officers, along with employees of Shanghai technology companies working at the direction of the SSSB, conspired to steal information through unauthorized access ("hacking") into computers in the United States and elsewhere, including by exploiting vulnerabilities in a certain Microsoft product as part of a mass intrusion campaign known publicly as "HAFNIUM." SSSB OFFICER 1 ("OFFICER 1") and SSSB OFFICER 2 ("OFFICER 2") directed defendants XU ZEWEI and ZHANG YU, together with their co-conspirators, to hack into or facilitate intrusions of university and business computers

located in the United States and elsewhere for the purpose of gaining and maintaining unauthorized access to those computers and stealing information. XU and ZHANG, together with their co-conspirators, including but not limited to OFFICER 1 and OFFICER 2, are collectively referred to in this Indictment as the "conspirators."

3. Beginning in early 2020, the conspirators targeted, among others, U.S.-based universities and leading immunologists and virologists conducting ground-breaking research into COVID-19 vaccines, treatments, and testing. Beginning in late 2020, the conspirators exploited certain vulnerabilities in Microsoft Exchange Server, a widely-used Microsoft product for sending, receiving, and storing email messages, to target a law firm and others with insight into the United States' government policies and policymakers. Months later, in a March 2, 2021 report, Microsoft publicly disclosed an intrusion campaign by state-sponsored hackers operating out of China, a group Microsoft named "HAFNIUM," which exploited these same vulnerabilities in Microsoft Exchange Server. The conspirators thus were at the forefront of the PRC's "HAFNIUM" intrusion campaign, which the United States government, the European Union, the United Kingdom, and the North Atlantic Treaty Organization, and private sector cybersecurity leaders later condemned as an "indiscriminate," "reckless," "irresponsible," and "destabilizing" hack of thousands of computers worldwide.

4. The conspirators included, but were not limited to:

a. XU ZEWEI, a general manager at Shanghai Powerock Network Co. Ltd. ("Powerock"), who operated at the direction of the SSSB. XU was a resident and citizen of the PRC. Among other things, XU worked on taskings from the SSSB, supervised hacking activity of other Powerock personnel in support of

such taskings, coordinated hacking activities with fellow hacker ZHANG YU, and reported the results of the hacking activities to the SSSB.

b. ZHANG YU, a director at Shanghai Firetech Information Science and Technology Company, Ltd. ("Firetech"), who operated at the direction of the SSSB. ZHANG was a resident and citizen of the PRC. Among other things, ZHANG worked on taskings from the SSSB, supervised hacking activity, including that of other Firetech personnel in support of such taskings, and coordinated hacking activities with fellow hacker XU.

c. OFFICER 1, an officer in the SSSB who supervised and directed hacking activities, including the theft of information, conducted by one or more members of the conspiracy. OFFICER 1 was a resident and citizen of the PRC. Among other things, OFFICER 1 oversaw the intrusion into UNIVERSITY 1, and XU's and ZHANG's work on the HAFNIUM intrusion campaign.

d. OFFICER 2, an officer in the SSSB who supervised and directed hacking activities, including the theft of information, conducted by one or more members of the conspiracy. OFFICER 2 was a resident and citizen of the PRC. Among other things, OFFICER 2 oversaw the intrusions into UNIVERSITY 1 and UNIVERSITY 2, and XU's and ZHANG's work on the HAFNIUM intrusion campaign.

5. The conspirators hacked into protected computers–that is, computers used in and affecting interstate and foreign commerce and communications–operated by the following universities and business, among others, to steal information:

a. UNIVERSITY 1, a university based in the Southern District of Texas engaged in, among other activities, research into COVID-19 vaccines, treatments, and testing,

b. UNIVERSITY 2, a university based in North Carolina engaged in, among other activities, research into COVID-19 vaccines, treatments, and testing,

c. UNIVERSITY 3, a university based in the Southern District of Texas, and

d. LAW FIRM, a law firm with offices in Washington, D.C., and other locations inside and outside the United States.

COUNT ONE

(Conspiracy to Cause Damage to and Obtain Information by Unauthorized Access to Protected Computers, to Commit Wire Fraud, and to Commit Aggravated Identity Theft)

6. The allegations in Paragraphs 1 through 5 of this Indictment are re-alleged here.

7. From in or around February 2020 through in or around June 2021, in the Southern District of Texas, and elsewhere within the jurisdiction of the Court:

XU ZEWEI
and
ZHANG YU,

the defendants, together with others known and unknown to the Grand Jury, did knowingly and intentionally conspire and agree to commit the following offenses against the United States:

a. Knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally caused damage without authorization to protected computers, resulting in loss during a one-year period aggregating at least $5,000 in value, and damage affecting ten or more protected computers in during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B)(i);

b. Intentionally access computers without authorization, and thereby obtained information from at least one protected computer, such conduct having involved an interstate and foreign communication, and the offense was committed for purposes of commercial advantage and private financial gain, was 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, and the information was valued greater than $5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B)(i), (ii) and (iii);

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

d. During and in relation to the crime of wire fraud, in violation of Title 18, United States Code, Section 1343, and the crime of obtaining information by unauthorized access to protected computers, in violation of Title 18, United States Code, Section 1030(a)(2)(C), did knowingly transfer, possess, and use without lawful authority, a means of identification of another person, in violation of Title 18, United States Code, Sections 1028A(a)(1), 1028A(b), and 1028A(c)(4), (5).

OBJECT OF THE CONSPIRACY

8. The object of the conspiracy was for the defendants and others known and unknown to the Grand Jury, acting from inside the PRC and on behalf of the SSSB, to obtain and maintain unauthorized access to the victims' computers and to accomplish the following objectives, among others, depending on the particular intrusion: (i) create and maintain illegal, unauthorized access to victims' computers; and (ii) steal the victims' data, including COVID-19 research, for the benefit of PRC-based entities and the strategic benefit of the PRC government.

MANNER AND MEANS OF THE CONSPIRACY

9. As part of the conspiracy, the conspirators supported one another, and aided and abetted computer hacking committed by one another, by sharing information about the victims and their computer networks, by sharing malware and information about malware, and by sharing tactics, techniques, and procedures for successfully committing computer intrusions targeting protected computers.

10. As part of the conspiracy, the conspirators exploited vulnerabilities in the victims' computers to gain and maintain unauthorized access to the victim computers and networks. Through this unauthorized access, the conspirators installed and accessed malware that allowed the conspirators to identify, collect, and exfiltrate information stored on the victim computers.

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

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

13. As part of the conspiracy, the conspirators in some instances also stole data from victims' computers, including COVID-19 research.

OVERT ACTS

14. In furtherance of the conspiracy and to effect the object thereof, the following overt acts, among others, were committed within the Southern District of Texas and elsewhere, on or about the dates below:

a. Intrusion Into, and Theft From, UNIVERSITY 1's Computers:

i. On or about February 17, 2020, XU and ZHANG discussed a certain known computer vulnerability (Common Vulnerability and Exposure ("CVE") 2019-11510). This vulnerability, among other things, allows hackers to read a computer's temporary memory to identify, and thereby steal, user account credentials.

ii. On or about February 19, 2020, the conspirators leased a virtual private server ("VPS 1") and used VPS 1 to download a script for deploying CVE-2019-11510.

iii. On or about February 19, 2020, the conspirators used VPS 1 to attempt to exploit a computer that is part of UNIVERSITY 1's virtual private network ("VPN") using CVE-2019-11510.

iv. On or about February 19, 2020, the conspirators accessed the same UNIVERSITY 1 VPN without authorization using stolen user account credentials. The conspirators maintained unauthorized access through at least May 7, 2020.

v. On or about February 19, 2020, XU provided OFFICER 2 with confirmation that he had compromised the UNIVERSITY 1 VPN.

vi. On or about February 19, 2020, ZHANG referred XU to information about the UNIVERSITY 1 VPN. ZHANG also referred XU to a list of account usernames for UNIVERSITY 1 employees. Among the usernames was the username for an account the conspirators used to access the UNIVERSITY 1 VPN.

vii. On or about February 20, 2020, OFFICER 1 directed XU to target UNIVERSITY 1 email accounts. OFFICER 1 then provided XU with information regarding the migration of UNIVERSITY 1 email accounts to Microsoft Office 365.

viii. Later, on or about February 20, 2020, OFFICER 2 provided XU with the same Microsoft Office 365 migration information that OFFICER 1 had provided earlier that day.

ix. On or about February 20 and February 21, 2020, the conspirators installed certain unauthorized services on UNIVERSITY 1 computers used for remote access and code execution.

x. Beginning on or about February 20, 2020, the conspirators accessed without authorization the email accounts ("mailboxes") of UNIVERSITY 1 employees, including the mailboxes of virologists and immunologists engaged in research into COVID-19 vaccines, treatment, and testing.

xi. On or about February 20, 2020, the conspirators executed an unauthorized command to steal the contents of specified UNIVERSITY 1 mailboxes. Several gigabytes of data were stolen from the UNIVERSITY 1 network.

xii. On or about February 21, 2020, XU and ZHANG discussed XU's acquisition of the contents of mailboxes.

xiii. On or about February 22, 2020, OFFICER 2 provided XU a list of five mailbox usernames and directed XU to steal the contents of the mailboxes. The usernames were the usernames of five UNIVERSITY 1 employees, including virologists and immunologists, engaged in COVID-19 research.

xiv. The conspirators accessed without authorization the mailboxes of these employees. On or about February 24, 2020, XU informed OFFICER 2 that he acquired the contents of the mailboxes.

xv. On or about April 13, 2020, OFFICER 2 directed XU to target UNIVERSITY 1 again, specifically identifying three UNIVERSITY 1 employees as targets. These three employees were virologists/immunologists engaged in COVID-19 research and had been previously targeted by the conspirators.

xvi. On or about April 14 and 15, 2020, the conspirators accessed without authorization the mailbox of at least one of these three targeted COVID-19 researchers.

xvii. Beginning on or about April 14, 2020, and continuing through on or about April 27, 2020, the conspirators stole data from the UNIVERSITY 1 network.

b. Intrusion Into UNIVERSITY 2's Computers:

i. On or about February 5, 2020, OFFICER 2 directed XU to conduct reconnaissance on UNIVERSITY 2's school of public health. XU agreed.

ii. On or about February 14, 2020, OFFICER 2 directed XU to conduct research on a professor at UNIVERSITY 2's school of public health who was engaged in COVID-19 research. XU agreed.

iii. On or about February 18, 2020, the conspirators used VPS 1 to conduct reconnaissance of domains and IP addresses associated with UNIVERSITY 2, including its school of public health.

iv. On or about February 18, 2020, the conspirators used VPS 1 to conduct vulnerability scanning of UNIVERSITY 2 computers.

v. On or about February 19 and 20, 2020, the conspirators used VPS 1 to attempt to exploit certain computers on UNIVERSITY 2's network using CVE-2019-19781.

c. Intrusion Into, and Theft From, UNIVERSITY 3's Computers:

i. On or about January 4, 2021, the conspirators installed an unauthorized web shell named "help.aspx" on a UNIVERSITY 3 computer running Microsoft Exchange Server. Web shells are pieces of code or scripts running on a computer that enable remote administration. At this time, this help.aspx web shell was not publicly known. The help.aspx web shell was later identified in the March 2, 2021 Microsoft report as being used by HAFNIUM actors.

ii. On or about January 5, 2021, XU and ZHANG discussed research into vulnerabilities in Microsoft Exchange Server. In particular, they discussed a

report that a certain researcher ("RESEARCHER 1") had identified a serious remote code execution vulnerability and speculated that it might concern Microsoft Exchange Server.

iii. On or about January 15, 2021, XU sent ZHANG a link to a file for a web shell known as the "TwoFace" web shell.

iv. On or about January 29, 2021, the conspirators installed unauthorized web shells "healthcheck.aspx" and "iisstart.aspx" on UNIVERSITY 3 computers running Microsoft Exchange Server. The iisstart.aspx web shell was a variant of the TwoFace web shell XU sent to ZHANG by link. At this time, these healthcheck.aspx and iisstart.aspx web shells were not publicly known. They were later identified in the March 2, 2021 Microsoft report as being used by HAFNIUM actors.

v. On or about January 30, 2021, XU confirmed to ZHANG that he (XU) had compromised the UNIVERSITY 3 computer network. In addition to identifying UNIVERSITY 3 by its name, XU informed ZHANG of the specific intrusion detection tool used by UNIVERSITY 3. XU discovered UNIVERSITY 3's use of this intrusion detection tool through his hacking of UNIVERSITY 3 computers.

vi. On or about February 1, February 24, and February 26, the conspirators accessed UNIVERSITY 3 computers running Microsoft Exchange Server via the unauthorized web shells help.aspx, healthcheck.aspx, and iisstart.aspx.

vii. On or about February 6, 2021, the conspirators attempted to access a UNIVERSITY 3 computer running Microsoft Exchange Server via an

unauthorized web shell named "errorEEE.aspx." At this time, the errorEEE.aspx web shell was not publicly known. The errorEEE.aspx web shell, as well as the "errorEE.aspx," "errorEW.aspx," and "errorFF.aspx" web shells, were later identified in the March 2, 2021 Microsoft report as being used by HAFNIUM actors.

viii. On or about February 27, 2021, OFFICER 1 confirmed to XU that their efforts were successful in multiple instances.

ix. On or about February 28, 2021, XU updated OFFICER 2 on the successful intrusions. OFFICER 2 directed XU to get a list of the successful intrusions from OFFICER 1. XU obtained the list.

x. On or about February 27 and February 28, 2021, the conspirators attempted to exploit UNIVERSITY 3 computers running Microsoft Exchange Server using a certain computer vulnerability (CVE-2021-26855). At the time the conspirators were using CVE-2021-26855, it was not publicly known; that is, it was a "zero-day" vulnerability. Microsoft reported on March 2, 2021, that CVE-2021-26855 was among the Microsoft Exchange Server vulnerabilities used by HAFNIUM actors.

xi. On or about March 2, 2021, the conspirators successfully exploited a UNIVERSITY 3 computer running Microsoft Exchange Server using a CVE-2021-26855.

xii. On or about March 2, 2021, the conspirators accessed UNIVERSITY 3 computers running Microsoft Exchange Server via the unauthorized HAFNIUM healthcheck.aspx web shell.

xiii. On or about March 3, 2021, ZHANG and XU discussed the March 2, 2021 Microsoft report on vulnerabilities in Microsoft Exchange Server and the solution ("patch") for fixing them.

d. Intrusion Into, and Theft From, LAW FIRM's Computers:

i. On or about October 23, 2020, XU and ZHANG discussed XU's plan to target a law firm and the fact that it had a certain multi-factor authentication that might make remote access difficult.

ii. On or about November 30, 2020, the conspirators installed an unauthorized web shell on one of the LAW FIRM's computers running Microsoft Exchange Server. The conspirators then expanded their unauthorized access to the LAW FIRM's network.

iii. On or about December 10, 2020, XU and ZHANG discussed XU's targeting of a law firm. ZHANG later provided XU with information regarding a certain Microsoft Exchange Server vulnerability known as CVE-2020-17144.

iv. From in or around December 2020 to in or around February 2021, the conspirators accessed without authorization the mailboxes of LAW FIRM attorneys and stole information from those mailboxes.

v. On or about January 4, 2021, the conspirators accessed without authorization the LAW FIRM's computers and conducted hundreds of searches of mailboxes for specific LAW FIRM attorneys and clients. The searches specifically searched for information on specific U.S. policy makers and government agencies. The search terms also included "Chinese sources," "MSS," and "HongKong."

vi. On or about January 5 and January 13, 2021, ZHANG and XU discussed a certain Microsoft Exchange Server vulnerability known as CVE-2020-0688.

vii. On or about January 15, 2021, the conspirators used CVE-2020-0688 to access without authorization one or more LAW FIRM computers running Microsoft Exchange Server.

viii. On or about January 15, 2021, via CVE-2020-0688, the conspirators installed unauthorized web shells named "OrgIdError.aspx" and "HybridLogout.aspx" on a LAW FIRM computer running Microsoft Exchange Server.

ix. On or about January 30, 2021, the conspirators installed the unauthorized iisstart.aspx HAFNIUM web shell on a LAW FIRM computer running Microsoft Exchange Server. As described above, the iisstart.aspx HAFNIUM web shell was a variant of the web shell XU sent to ZHANG by link. This web shell was installed on a LAW FIRM computer running Microsoft Exchange Server approximately one day after the conspirators installed the iisstart.aspx web shell on a UNIVERSITY 3 computer running Microsoft Exchange Server. At the time of installation at both UNIVERSITY 3 and LAW FIRM, this iisstart.aspx web shell was not publicly known.

x. On or about March 17, 2021, the conspirators conducted additional searches of LAW FIRM mailboxes.

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

COUNT TWO
(Conspiracy to Commit Wire Fraud)

15. The allegations contained in Paragraphs 1 through 5 and Paragraphs 9 through 14 of this Indictment are re-alleged here.

16. From in or around February 2020 through in or around June 2021, in the Southern District of Texas, and elsewhere within the jurisdiction of the Court:

XU ZEWEI
and
ZHANG YU,

the defendants, unlawfully and knowingly did combine, conspire, confederate and agree together, and with each other and others known and unknown to the Grand Jury, to violate Title 18, United States Code, Section 1343.

17. It was a part and an object of the conspiracy that the defendants, and others known and unknown to the Grand Jury, having devised and intended to devise a scheme and artifice to defraud and for obtaining money and property by false and fraudulent pretenses, representations or promises, would and did transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, and pictures for the purpose of executing such scheme and artifice; to wit, the defendants knowingly and fraudulently communicated by means of wires with computers belonging to UNIVERSITY 1, UNIVERSITY 2, UNIVERSITY 3, and LAW FIRM to create and maintain unauthorized access to those computers and to obtain proprietary and valuable information from UNIVERSITY 1, UNIVERSITY 2, UNIVERSITY 3, and LAW FIRM.

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

COUNT THREE
(Wire Fraud)

18. The allegations contained in Paragraphs 1 through 5 and Paragraphs 8 through 14 of this Indictment are re-alleged here.

19. On or about February 19, 2020, and continuing on until at least May 7, 2020, in the Southern District of Texas and elsewhere within the jurisdiction of the Court:

XU ZEWEI
and
ZHANG YU,

the defendants, aiding and abetting each other and others known and unknown to the Grand Jury, and having devised and intending to devise a scheme and artifice to defraud, and to obtain property by means of false and fraudulent pretenses, representations and promises, transmitted and caused to be transmitted by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, and pictures for the purpose of executing such scheme and artifice; to wit, the defendants knowingly and fraudulently communicated by means of wires with computers belonging to UNIVERSITY 1 to create and maintain unauthorized access to those computers and to obtain proprietary and valuable information from UNIVERSITY 1.

In violation of Title 18, United States Code, Sections 1343 and 2.

COUNT FOUR
(Wire Fraud)

20. The allegations contained in Paragraphs 1 through 5 and Paragraphs 8 through 14 of this Indictment are re-alleged here.

21. On or about January 4, 2021, and continuing on until at least March 2, 2021, in the Southern District of Texas and elsewhere within the jurisdiction of the Court:

XU ZEWEI
and
ZHANG YU,

the defendants, aiding and abetting each other and others known and unknown to the Grand Jury, and having devised and intending to devise a scheme and artifice to defraud, and to obtain property by means of false and fraudulent pretenses, representations and promises, transmitted and caused to be transmitted by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, and pictures for the purpose of executing such scheme and artifice; to wit, the defendants knowingly and fraudulently communicated by means of wires with computers belonging to UNIVERSITY 3 to create and maintain unauthorized access to those computers and to obtain proprietary and valuable information from UNIVERSITY 3.

In violation of Title 18, United States Code, Sections 1343 and 2.

COUNT FIVE
(Obtaining Information by Unauthorized Access to Protected Computers)

22. The allegations contained in Paragraphs 1 through 5 and Paragraphs 8 through 14 of this Indictment are re-alleged here.

23. From on or about February 19, 2020, and continuing on until at least May 7, 2020, in the Southern District of Texas, and elsewhere within the jurisdiction of the Court:

XU ZEWEI
and
ZHANG YU,

the defendants, aiding and abetting each other and others known and unknown to the Grand Jury, intentionally accessed, caused to intentionally access, and attempted to intentionally access without authorization a computer used in interstate and foreign commerce and thereby obtained information from a protected computer, namely the computer network of UNIVERSITY 1, and (1) the offense was committed for purposes of commercial advantage and private financial gain,

(2) the offense was committed 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 18 U.S.C. § 1343, and (3) the information obtained from a protected computer belonging to UNIVERSITY 1 had value in excess of $5,000.

In violation of Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(B)(i), (ii) and (iii) and 2.

COUNT SIX

(Obtaining Information by Unauthorized Access to Protected Computers)

24. The allegations contained in Paragraphs 1 through 5 and Paragraphs 8 through 14 of this Indictment are re-alleged here.

25. From on or about January 4, 2021, and continuing on until at least March 2, 2021, in the Southern District of Texas, and elsewhere within the jurisdiction of the Court:

XU ZEWEI
and
ZHANG YU,

the defendants, aiding and abetting each other and others known and unknown to the Grand Jury, intentionally accessed, caused to intentionally access, and attempted to intentionally access without authorization a computer used in interstate and foreign commerce and thereby obtained information from a protected computer, namely the computer network of UNIVERSITY 3, and (1) the offense was committed for purposes of commercial advantage and private financial gain, and (2) the offense was committed 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 18 U.S.C. § 1343.

In violation of Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(B)(i), (ii) and (iii) and 2.

COUNT SEVEN
(Intentional Damage to a Protected Computer)

26. The allegations contained in Paragraphs 1 through 5 and Paragraphs 8 through 14 of this Indictment are re-alleged here.

27. From on or about February 19, 2020, and continuing on until at least May 7, 2020, in the Southern District of Texas, and elsewhere within the jurisdiction of the Court:

XU ZEWEI
and
ZHANG YU,

the defendants, aiding and abetting each other and others known and unknown to the Grand Jury, knowingly caused and attempted to cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally caused damage without authorization to protected computers belonging to UNIVERSITY 1. The offense caused loss to one or more persons resulting from a related course of conduct affecting one or more protected computers aggregating at least $5,000 in value, and damage affecting ten or more protected computers during a one-year period.

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

COUNT EIGHT
(Intentional Damage to a Protected Computer)

28. The allegations contained in Paragraphs 1 through 5 and Paragraphs 8 through 14 of this Indictment are re-alleged here.

29. From on or about January 4, 2021, and continuing on until at least March 2, 2021, in the Southern District of Texas, and elsewhere within the jurisdiction of the Court:

XU ZEWEI
and
ZHANG YU,

the defendants, aiding and abetting each other and others known and unknown to the Grand Jury, knowingly caused and attempted to cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally caused damage without authorization to protected computers belonging to UNIVERSITY 3. The offense caused loss to one or more persons resulting from a related course of conduct affecting one or more protected computers aggregating at least $5,000 in value.

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

COUNT NINE
(Aggravated Identity Theft)

30. The allegations contained in Paragraphs 1 through 5 and Paragraphs 8 through 14 of this Indictment are re-alleged here.

31. On or about February 19, February 20, February 21, February 23, March 19, and March 20, 2020, in the Southern District of Texas, and elsewhere within the jurisdiction of the Court:

XU ZEWEI
and
ZHANG YU,

the defendants, aiding and abetting each other and others known and unknown to the Grand Jury, knowingly transferred, possessed and used without lawful authority, a means of identification of another person, namely T.H., M.H., C.K., A.C., and A.R., employees of UNIVERSITY 1, 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)(C).

In violation of Title 18, United States Code, Sections 1028A(a)(1), (c)(4), (5) and 2.

NOTICE OF CRIMINAL FORFEITURE

Pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i), the United States gives notice that upon conviction of a computer fraud count as charged in the Indictment, the United States will seek forfeiture of all property, real or personal, which constitutes or is derived from proceeds traceable to such offenses; and any personal property that was used or intended to be used to commit or to facilitate the commission of such violation.

Pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), the United States gives notice that upon conviction of a Section 1349 or 1343 offense as charged in the Indictment, the United States will seek forfeiture of all property, real or personal, which constitutes or is derived from proceeds traceable to such offenses.

If any of the property described above as being subject to forfeiture, 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 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 defendants shall forfeit to the United States any other property of the defendants, up to the value of the property described above, pursuant to 21 U.S.C. § 853(p).

A TRUE BILL

Original Signature on File

GRAND JURY FOREPERSON

Alamdar S. Hamdani
United States Attorney
Southern District of Texas

By: _____
S. Mark McIntyre
Assistant United States Attorney
Southern District of Texas

Matthew G. Olsen
Assistant Attorney General
National Security Division

By: _____
Matthew A. Anzaldi
Trial Attorney
U.S. Department of Justice
National Security Division
National Security Cyber Section