IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	
	)	Criminal No. 17-247
v.	)	
	)	
	)	18 U.S.C. §§ 1030(a)(2)(C), 1030(a)(5)(A), 1030(b)
WU YINGZHUO	)	
a/k/a "mxmtmw"	)	18 U.S.C. § 1832(a)(1), 1832(a)(2), 1832(a)(5)
a/k/a "Christ Wu"	)	
a/k/a "wyz"	)	18 U.S.C. § 1343
DONG HAO	)	18 U.S.C. § 1028A
a/k/a "Bu Yi"	)	
a/k/a "Dong Shi Ye"	)	
a/k/a "Tianyu,"	)	**UNDER SEAL**
XIA LEI	)	
a/k/a "Sui Feng Yan Mie"	)	

INDICTMENT

The grand jury charges:

1. At all times relevant to the indictment:

BOYUSEC

a. The defendants were owners, employees and associates of the Guangzhou Bo Yu Information Technology Company Limited (hereinafter "Boyusec").

b. Boyusec purported to be a Chinese cybersecurity firm located at 1103 West Tower, Huapu Plaza, Number 9, Huaming Road, Pearl River New City, Tianhe District, Guangzhou, Guangdong Province, China.

c. According to its website, www.boyusec.com, Boyusec provided cybersecurity services for Chinese companies, including "Information Security and Testing," "Software Development and Testing," and "Data Analysis," in partnership with a large Chinese telecommunications company and another cybersecurity center in Guangdong Province.

d. In or around November 2013, Boyusec was registered as a limited liability company with the Tianhe Branch of the Guangzhou Administration for Industry and Commerce.

THE DEFENDANTS

e. Defendant WU YINGZHUO ("WU") was a resident of Guangzhou and used the aliases "mxmtmw," "Christ Wu," and "wyz." WU was a founding member and equity shareholder of Boyusec.

f. Defendant DONG HAO ("DONG") was a resident of Guangzhou and used the aliases "Bu Yi," "Dong Shi Ye," and "Tianyu." DONG was a founding member, equity shareholder of Boyusec, and held the title of "Executive Director and Manager"of Boyusec.

g. Defendant XIA LEI ("XIA") was a resident of Guangzhou and used the alias "Sui Feng Yan Mie." XIA was an employee of Boyusec.

THE U.S. VICTIMS

h. Moody's Analytics was an economic analysis firm which provided financial and economic services. Moody's Analytics employs economists, modelers and statisticians and primarily serves asset managers, banks, corporations, and insurers. Specifically, Moody's Analytics provided tools and information for measuring and managing risk through its expertise in credit analysis, economic research, and financial risk management. Moody's Analytics is headquartered in New York, New York.

i. Siemens AG ("Siemens") is a multinational manufacturing and electronics conglomerate, specializing in financial services, building technologies, mobility operations, healthcare, transportation, digitalization, power generation, power systems, and energy management. Siemens employs over 375,000 employees located in over 200 countries. Siemens is headquartered in Germany and had offices located in the Western District of Pennsylvania.

j. Trimble Inc, formerly known as Trimble Navigation Limited ("Trimble"), is a manufacturer, developer, and provider of geospatial positioning technology, including Global Positioning System (GPS) and Global Navigation Satellite Systems (GNSS) technology and related software and services, which are used in a variety of commercial industries, including the construction, land survey, and agricultural sectors. Trimble's products are sold and used in over 150 countries around the world. Trimble's innovations in positioning technology have resulted in over 1,200 patents. Trimble is headquartered in Sunnyvale, California.

COUNT ONE
(Conspiracy to Commit Computer Fraud and Abuse)

2. Beginning no later than 2011, and continuing until at least May 2017, in the Western District of Pennsylvania and elsewhere, the defendants,

WU YINGZHUO
a/k/a "mxmtmw"
a/k/a "Christ Wu"
a/k/a "wyz"
DONG HAO
a/k/a "Bu Yi"
a/k/a "Dong Shi Ye"
a/k/a "Tianyu," and
XIA LEI
a/k/a "Sui Feng Yan Mie"

did knowingly and willfully conspire and agree together, with each other, and with others known and unknown to the grand jury, to commit computer fraud and abuse, namely:

a) to access computers without authorization and exceed authorized access to computers, and to obtain thereby information from protected computers, for the purpose of commercial advantage and private financial gain, in furtherance of a criminal and tortious act in violation of the laws of the Commonwealth of Pennsylvania, namely, the common law tort of Invasion of Privacy, and where the value of the information did, and would if completed, exceed

$5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B)(i)-(iii); and

b) to cause the transmission of programs, codes, and commands, and as a result of such conduct, to cause damage without authorization to protected computers and where the offense did cause and would, if completed, have caused, loss aggregating $5,000 in value to at least one person, during a one-year period from a related course of conduct affecting a protected computer, and damage affecting at least 10 protected computers during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B).

MANNER AND MEANS OF THE CONSPIRACY

3. It was part of the conspiracy that defendants WU, DONG, XIA, and others known and unknown to the grand jury (collectively, "the co-conspirators"), agreed to participate in coordinated, and unauthorized targeted cyber-intrusions against businesses and entities, operating in the United States and elsewhere, in order to steal confidential business information and intentionally cause damage to those victims' computer systems.

4. The co-conspirators exploited vulnerabilities in computer systems or used malware, or malicious code to obtain and maintain unauthorized access into computers in order to steal hundreds of gigabytes of data, including confidential business and commercial information, work product, and sensitive victim employee information, such as usernames and passwords.

5. The co-conspirators attempted to hide their true identities and location by using aliases and intermediary computer servers known as "hop points." The co-conspirators compromised the hop points, which were private computer networks owned by third parties, and used these networks without authorization. By using the hop points, the co-conspirators misrepresented their true Internet Protocol ("IP") addresses, location, and identities to the victims and used the hop points for the purpose of identifying, collecting, packaging, and stealing data

from the victims. In order to thwart identification, the co-conspirators also used aliases when registering for online communications services.

SPEARPHISHING EMAILS

6. The co-conspirators used spearphishing campaigns to gain unauthorized access to the computer networks of U.S. and foreign businesses. The conspirators sent, and caused to be sent, spearphishing emails to computers located in the Western District of Pennsylvania and around the world.

7. The spearphishing emails misrepresented the identity of the sender, the subject matter of the email, and nature of any links or files contained within or attached to the email. In fact, many of the emails contained fraudulent links to either (a) computer files that contained malware that provided unauthorized access to the recipient's computer (known as a "backdoor"), thereby allowing the co-conspirators to bypass normal authentication procedures on the recipient's computer; or (b) servers' software designed to scan for vulnerabilities on the computers that connect to them.

MALWARE

8. The co-conspirators used different types of customized malware to gain and maintain unauthorized access into the computer networks. In order to initially access the victims' networks, the co-conspirators typically used a backdoor designed to bypass the victims' security systems and firewalls. The co-conspirators also commonly used malware referred to as "ups" and "exeproxy" (collectively "the UPS Backdoor Malware") to remotely access and control infected computers within the victims' networks. Specifically, the co-conspirators used multiple versions of UPS Backdoor Malware to misrepresent their status as authorized users of the victims' computers in order to issue commands to search, identify, copy, package and steal data stored on such computers.

CONCEALMENT

9. Beginning no later than 2013, and during their employment at Boyusec, defendants WU, DONG, XIA and others, known and unknown to the grand jury, worked together to conduct targeted cyberattacks against U.S. and foreign businesses which had never retained Boyusec for any services or otherwise authorized access into their computer networks.

10. Defendants WU, DONG, and XIA shared access to common hop points in order to conceal their identities, location, and affiliation with Boyusec during the course of their cyberattacks.

11. Defendants WU and DONG used stolen network credentials to conceal their unauthorized access to victim computer networks from the victims' security measures.

TARGETED ATTACKS OF U.S. BUSINESSES

Moody's Analytics

12. In 2005, Moody's Analytics purchased an economic analytics company that employed an influential economist who had expertise in macroeconomics and the housing finance sector ("Employee A"). Employee A became a public figure in the industry and was viewed by Moody's Analytics as a branding asset. Employee A commonly appeared on national TV and in newspapers with large circulations.

13. Beginning no later than 2011, the co-conspirators placed a forwarding rule on a Moody's Analytics email server directing all of Employee A's incoming emails to forward to co-conspirator-controlled web-based email accounts ("the Fraudulent Email Accounts").

14. Between June 21, 2013 and January 31, 2014, defendant XIA accessed a Fraudulent Email Account and its contents. These emails contained, among other things, Employee A's communications, which contained proprietary and confidential economic analyses, findings, and opinions.

Siemens

15. In 2014, Siemens was an international conglomerate servicing multiple industry sectors, including financial services, building technologies, mobility operations, healthcare, transportation, digitalization, power generation, power systems, and energy management.

16. In May and June 2014, the co-conspirators used hop points to target and gain unauthorized access to Siemens' computer networks for the purpose of obtaining and using Siemens employees' usernames and passwords and to steal proprietary commercial data.

17. In June 2014, defendant DONG accessed the Siemens' computer network, in the Western District of Pennsylvania and elsewhere, using UPS Backdoor Malware, and exfiltrated computer password information known as "hashes."

18. From approximately June 2015 to August 2015, the conspirators removed approximately 407GB of data from Siemens's network. The data included files and data created by Siemens' energy, technology, and transportation businesses.

Trimble

19. In 2015 and 2016, Trimble was engaged in the development of a new GNSS product that combined software with a relatively low cost antenna to significantly improve the positioning accuracy of mobile devices, including tablets and mobile telephones ("the Commercial GNSS Project"). The Commercial GNSS Project allowed Trimble customers to receive and process (a) GNSS satellite signals, and (b) data from Trimble's subscription corrections services. Using the data received from the GNSS satellites and Trimble's proprietary corrections services, users could obtain high precision position accuracy up to a few centimeters in a cost effective manner. Trimble's targeted customer markets for the Commercial GNSS Project were, among others, the construction, land survey, and agricultural sectors. The Commercial GNSS Project had no military applications.

20. This Commercial GNSS Project had been in development for approximately three years and had represented an investment of millions of dollars by Trimble. As such, Trimble's computer networks contained documents and other data pertaining to both the Commercial GNSS Project's technical development and the business and marketing strategy. Access to certain documents and data were restricted by Trimble based on a need to know. In addition, Trimble required that its employees and contractors sign Non-Disclosure Agreements to protect the development of the Commercial GNSS Project.

21. Beginning no later than December 2015 and continuing through March 2016, the co-conspirators targeted the servers within Trimble's network, including those that hosted documents and data relating to the Commercial GNSS Project.

22. Beginning no later than January 11, 2016, defendant WU accessed Trimble's network and copied, packaged, and stole computer files containing commercial business documents and data relating to the Commercial GNSS Project. Specifically, on January 11, 2016, WU prepared a zip archive file containing approximately 252 megabytes of compressed data from Trimble's network and removed the file from the network. This zip file contained hundreds of files of Trimble's technical, design, and business marketing documents pertaining to the Commercial GNSS Project.

23. The stolen zip file contained files marked "confidential" or "proprietary," and contained market research and strategy for the Commercial GNSS Project, which were a trade secret and commercial in nature ("Trade Secret 1" and "Trade Secret 2"). Trade Secret 1 and Trade Secret 2 contained confidential information regarding Trimble's market share, costs of production, and a timetable for the release and marketing of the Commercial GNSS Project.

24. The stolen zip file also contained a confidential and proprietary schematic design for the hardware receiver equipment component of the Commercial GNSS Project ("Trade Secret 3").

25. On or about January 12, 2016, a co-conspirator accessed Trimble's network and stole an additional 23 megabytes of data, including testing data for Trimble's proprietary subscription services.

26. This stolen data included confidential testing data of Trimble technology ("Trade Secret 4").

27. On or about January 22, 2016, the co-conspirators accessed Trimble's network and executed commands to steal two directory lists. One of these directory lists included, listed files containing the name of a Trimble engineer and related to the Commercial GNSS Project.

28. In total, conspirators stole at least 275 megabytes of data, including compressed data, which included hundreds of files that would have assisted a Trimble competitor in developing, providing, and marketing similar software and subscription services, without incurring millions of dollars in research and development costs.

OVERT ACTS

29. In furtherance of the conspiracy, and to effect the objects of the conspiracy, the defendants and others, both known and unknown to the grand jury, committed the following overt acts:

a. On or about August 26, 2011, a co-conspirator created a Fraudulent Email Account in the name of Employee A of Moody's Analytics.

b. On or about August 26, 2011, the exact date being unknown, a co-conspirator accessed the mail server within the Moody's Analytics computer network and placed a forwarding rule on the server directing all emails sent to Employee A to be forwarded to the Fraudulent Email Account.

c. On or about June 21, 2013, defendant XIA accessed emails which had been forwarded to Employee A's fraudulent account.

d. On or about January 21, 2014, defendant XIA accessed a hop point and logged into a Fraudulent Email Account and accessed emails which had been forwarded from Employee A's email account.

e. On or about June 6, 2014, defendant DONG accessed a Siemens computer with hostname D**********V without authorization.

f. On or about June 6, 2014, defendant DONG transferred a file containing Siemens password hashes among computers within the Siemens network and attempted to decrypt some of those hashes.

g. On or about June 6, 2014, defendant DONG connected to host P*******A, a Siemens network computer located in the Western District of Pennsylvania and attempted to log in as a network administrator using stolen credentials.

h. On or about June 7, 2014, defendant DONG attempted to log on to Siemens host computer N******A using stolen credentials belonging to Siemens employee "P.P."

i. On or about June 7, 2014, defendant DONG attempted to log on to Siemens host computer N******A using stolen credentials belonging to Siemens employee "B.R."

j. On or about December 18, 2015, defendant WU accessed a hop point and then further accessed a Trimble computer with hostname W****M.

k. On or about December 26, 2015, a co-conspirator accessed a hop point and accessed Internet web pages of Trimble.

l. On or about January 9, 2016, defendant WU possessed and used the stolen credentials of Trimble employee "K.B" in order to connect to a Trimble computer at IP address 10.**.***.**8.

m. On or about January 11, 2016, defendant WU entered a series of commands resulting in the theft of approximately 773 files containing trade secrets and other proprietary information from Trimble's computer network.

n. On or about January 11, 2016, defendant WU entered a command to delete a log file named "Log.zip" from a computer within the Trimble network.

o. On or about January 12, 2016, a co-conspirator stole approximately four files containing proprietary information from the computer network of Trimble.

p. On or about January 14, 2016, defendant WU attempted to log into a Trimble computer using stolen credentials belonging to Trimble employee "R.M."

q. On or about January 22, 2016, defendant WU used stolen credentials belonging to Trimble employee "B.M." to gain unauthorized access to Trimble's computers.

In violation of Title 18, United States Code, Section 1030(b).

COUNT TWO
(Conspiracy to Commit Trade Secret Theft)

The grand jury further charges:

30. Paragraphs 1-29 of this indictment are incorporated herein as if set forth in full.

31. Beginning at least in or about 2011, and continuing until at least May 2017, in the Western District of Pennsylvania and elsewhere, the defendants,

WU YINGZHUO
a/k/a "mxmtmw"
a/k/a "Christ Wu"
a/k/a "wyz"
DONG HAO
a/k/a "Bu Yi"
a/k/a "Dong Shi Ye"
a/k/a "Tianyu," and
XIA LEI
a/k/a "Sui Feng Yan Mie"

did knowingly conspire and agree together and with each other, and with other persons both known and unknown to the grand jury, to copy, duplicate, download, upload, replicate, transmit, deliver, send, mail, communicate, and convey trade secrets without authorization that were related to products or services used in or intended for use in interstate and foreign commerce, with the intent to convert the trade secrets to the economic benefit of someone other than the owner of the trade secrets and with the intent and knowledge that the offense would injure the owner of the trade secrets, in violation of Title 18, United States Code, Section 1832(a)(1) and (2).

OVERT ACTS

32. In furtherance of the conspiracy, and to effect the objects of the conspiracy, the defendants and their co-conspirators, committed the overt acts alleged in paragraph 29.

In violation of Title 18, United States Code, Section 1832(a)(5).

COUNT THREE
(Wire Fraud)

The grand jury further charges:

33. Paragraphs 1-29 of this indictment are incorporated herein as if set forth in full.

34. Beginning no later than 2011, and continuing until at least May 2017, in the Western District of Pennsylvania and elsewhere, the defendants,

WU YINGZHUO
a/k/a "mxmtmw"
a/k/a "Christ Wu"
a/k/a "wyz"
DONG HAO
a/k/a "Bu Yi"
a/k/a "Dong Shi Ye"
a/k/a "Tianyu," and
XIA LEI
a/k/a "Sui Feng Yan Mie"

did devise, intend to devise, and participate in a scheme, with others known and unknown to the grand jury, to defraud and to obtain money and property by means of materially false and fraudulent pretenses and representations, and by concealment of materials facts.

35. It was part of the scheme that defendants used hop points to misrepresent their true IP address, location, and identities.

36. It was further part of the scheme that the defendants used the Fraudulent Email Accounts in order to misrepresent to the Moody's Analytics network that Employee A's emails were being forwarded to Employee A's personal email account when, in fact, the emails were forwarded to the Fraudulent Email Accounts.

37. It was further part of the scheme that the defendants used stolen credentials to gain access to parts of the victims' networks.

38. It is further part of the scheme that the defendants sought and stole internal and proprietary information belonging to commercial entities.

39. On or about June 6, 2014, in the Western District of Pennsylvania, and elsewhere, the defendants, for the purpose of executing the scheme to defraud, knowingly caused to be transmitted by means of wire communication in interstate commerce certain writings, signs, and signals, namely, an electronic signal containing credentials to a Siemens network computer.

In violation of Title 18, United States Code, Section 1343.

COUNTS FOUR THROUGH EIGHT
(Aggravated Identity Theft)

The grand jury further charges:

40. Paragraphs 1-29 are incorporated herein as if set forth in full.

41. Beginning at least on or about June 6, 2014, and continuing until at least January 22, 2016, in the Western District of Pennsylvania and elsewhere, the defendants,

WU YINGZHUO
a/k/a "mxmtmw"
a/k/a "Christ Wu"
a/k/a "wyz"
DONG HAO
a/k/a "Bu Yi"
a/k/a "Dong Shi Ye"
a/k/a "Tianyu," and
XIA LEI
a/k/a "Sui Feng Yan Mie"

aided and abetted by others known and unknown to the grand jury, during and in relation to the crime of conspiracy to commit computer fraud and abuse in violation of Title 18, United States Code, Section 1030(b) and wire fraud, in violation of Title 18, United States Code, Section 1343, as more fully set forth in Counts One and Three above, did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person.

42. On or about the dates identified in Column B of the chart set forth below, each date constituting a separate count as set forth in Column A, defendants did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, listed by initials in Column C, who was associated with a victim listed in Column D.

A Count	B Date (On or About)	C Means of Identification Belonging to	D Victim
4	June 6, 2014	P.P.	Siemens
5	June 7, 2014	B.R.	Siemens
6	January 9, 2016	K.B.	Trimble
7	January 14, 2016	R.M.	Trimble
8	January 22, 2016	B.M.	Trimble

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

A true bill,

~~FOREP~~PERSON

SOO C. SONG
Acting United States Attorney
DC ID No. 457268