SEALED

FILED
May 28 2021
2:50 pm
CLERK, U.S. DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA
BY s/ emilybl DEPUTY

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

November 2019 Grand Jury

UNITED STATES OF AMERICA,

Plaintiff,

v.

DING XIAOYANG (丁晓阳) (1),
aka Ding Hao,
aka Manager Chen,
CHENG QINGMIN (程庆民) (2),
aka Manager Cheng,
ZHU YUNMIN (朱允敏) (3),
aka Zhu Rong,
WU SHURONG (吴淑荣) (4),
aka goodperson,
aka ha0r3n,
aka Shi Lei,

Defendants.

Case No. '21 CR1622 GPC

INDICTMENT

Title 18, U.S.C., Secs. 371, 1030(a)(2)(B) and (C), 1030(c)(2)(B)(i) and (iii), 1030(a)(5)(A), and 1030(c)(4)(B)(i) - Conspiracy to Damage Protected Computers; Title 18, U.S.C., Sec. 1831(5) – Conspiracy to Commit Economic Espionage; Title 18, U.S.C., Sec. 982(a)(1) and (b)(1) – Criminal Forfeiture

FAS:nlv(2):San Diego:5/28/21

The grand jury charges:

Count 1

At various times relevant to this indictment:

INTRODUCTION

1. The Hainan Province Ministry of State Security ("HSSD") was a provincial foreign intelligence arm of the People Republic of China's ("PRC" or "China") Ministry of State Security ("MSS"). The MSS, and by extension the HSSD, was primarily responsible for domestic counterintelligence, non-military foreign intelligence, and aspects of political and domestic security.

2. Hainan was China's southernmost province and included Hainan Island, which was located in the South China Sea near Cambodia, Vietnam, Malaysia, and the Philippines, and home to the Yulin Naval Base.

3. In 2011, the HSSD created a front company, Hainan Xiandun Technology Development Co., Ltd. ("海南仙盾") ("Hainan Xiandun"), which held itself out publically as "a fast-growing high-tech information security company ... located in Haikou City, Hainan Province," providing "big data security, security situational awareness, and security technology research ... committed to exploring the development trend of cutting-edge science and technology."

4. From 2011 through at least 2018, a time period that in part post-dates the September 2015 commitment by China's President that the PRC government would not conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to PRC companies or commercial sectors, Hainan Xiandun employed hackers who sought to and did steal such data from companies and universities involved in virus and vaccine research of the Ebola virus and maritime research and development. Such trade secrets and confidential business included sensitive technologies used for submersibles and autonomous vehicles, specialty chemical formulas, and proprietary genetic-sequencing technology. Much of the stolen data would, among other things, provide a commercial and

strategic advantage to the PRC government, state-owned companies, and commercial sectors. Hainan Xiandun employed hackers also sought to and did steal data from U.S. and foreign government entities, in some instances for use to support the PRC's efforts to secure contracts for state-owned enterprises in the relevant countries. Security researchers tracked these Hainan Xiandun intrusions using the threat labels "APT40," "BRONZE MOHAWK," "FEVERDREAM," "G0065," "Gadolinium," "GreenCrash," "Hellsing," "Kryptonite Panda," "Leviathan," "MUDCARP," "Periscope," "Temp.Periscope," and "Temp.Jumper."

5. Hainan Xiandun employees, under the direction of HSSD intelligence officers, hacked or attempted to hack dozens of victims in the United States, Austria, Cambodia, Canada, Germany, Indonesia, Malaysia, Norway, Saudi Arabia, South Africa, Switzerland, and the United Kingdom, as well as others.

6. HSSD intelligence officers, including defendants DING XIAOYANG, CHENG QINGMIN, and ZHU YUNMIN, oversaw and directed the activities of Hainan Xiandun linguists and computer hackers, including defendant WU SHURONG.

7. Members of the conspiracy, including defendants DING XIAOYANG, CHENG QINGMIN, and ZHU YUNMIN, coordinated with staff and professors at various universities in Hainan and elsewhere in China to support and manage Hainan Xiandun as a front company for the HSSD, to identify and recruit talented computer hackers to penetrate foreign entities (including foreign universities) and steal trade secrets, proprietary research and data, and to identify and recruit talented linguists to interpret the stolen material.

8. The object of the conspiracy was to install malware and hacking tools on protected computers and to leverage such malware and tools to commit unauthorized computer intrusions, all with the goal of stealing information of value from foreign governments, universities, and companies on behalf of the PRC and its instrumentalities, including state-owned enterprises in the railway and shipbuilding industries, and PRC state-sponsored and private sector biopharmaceutical and other companies.

//

9. Members of the conspiracy included, but were not limited to:

a. Defendant DING XIAOYANG, aka Ding Hao, aka Manager Chen, was an MSS Intelligence Officer working in the HSSD, who has been recognized for his leadership by the MSS while supervising, facilitating, and managing computer hackers and linguists working at Hainan Xiandun for the benefit of the PRC and its state-owned and sponsored instrumentalities;



b. Defendant CHENG QINGMIN, aka Manager Cheng, was an MSS Intelligence Officer working in the HSSD, who supervised, facilitated, and managed computer hackers and linguists working at multiple MSS front companies for the benefit of the PRC and its various state-owned and sponsored instrumentalities;

c. Defendant ZHU YUNMIN, aka Zhu Rong, was an MSS Intelligence Officer working in the HSSD, who supervised, facilitated, and coordinated computer hackers working at Hainan Xiandun for the benefit of the PRC; and



d. Defendant WU SHURONG, aka goodperson, aka ha0r3n, aka Shi Lei, was a computer hacker who, as part of his job duties at Hainan Xiandun, created malware, hacked into computer systems operated by foreign governments, companies, and universities, and supervised other employees involved in Hainan Xiandun's hacking activities.



10. Members of the conspiracy hacked, and attempted to hack, into protected computers, that is, computers used in and affecting interstate and foreign commerce and communications, operated by the following government organizations, companies, and universities, among others, to steal information, including proprietary research, trade secrets or other confidential business information, and to use these institutions' computers to facilitate further computer intrusions:

a. Research Facility A – a research facility in California and Florida involved in the research and development of virus treatments and vaccines;

b. University A – a California university with a research institute involved in maritime and hydroacoustic research and development as well as a school of medicine;

c. University B – a Pennsylvania university with a robotics engineering program involved in the research and development of autonomous vehicles and maritime craft;

d. University C – a Hawaii university with an Applied Research Laboratory involved in maritime research and development;

e. University D – a Pennsylvania university involved in maritime research and development;

f. University E – a Maryland university with an Applied Physics Laboratory;

g. University F – a Texas university involved in maritime research and development;

h. University G – a Washington university with an Applied Physics Laboratory involved in maritime research and development;

i. Company A – a California information technology company;

j. Company B – a United States defense contractor headquartered in California, which is involved in maritime research and development;

k. Company C – a mid-Atlantic company involved in the manufacture of aircraft and marine craft;

l. Company D – a Swiss chemicals company, whose products include maritime paints;

m. Company E – an aircraft servicing company headquartered in New Jersey with repair and maintenance services at airports around the world;

n. Company F – an American airline;

o. Company G – a German industrial conglomerate with hundreds of subsidiaries around the world;

p. Company H – a United States defense contractor headquartered in Virginia, which is involved in maritime research and development.

q. A Cambodian government ministry ("Cambodian Government Ministry A");

r. Two Saudi Arabian government ministries ("Saudi Arabian Government Ministries A and B");

s. A Malaysian high-speed rail corporation ("Malaysian Rail Corporation A");

t. A Malaysian political party ("Malaysian Political Party A"); and

u. The National Institutes of Health ("NIH").

11. From a date unknown, but no later than July 2009, up to and including September 2018, within the Southern District of California, and elsewhere, defendants DING XIAOYANG, aka Ding Hao, aka Manager Chen, CHENG QINGMIN, ZHU YUNMIN, aka Zhu Rong, and WU SHURONG aka goodperson, aka ha0r3n, aka Shi Lei, did knowingly and intentionally conspire with each other and other persons known and unknown to the grand jury to commit an offense against the United States, that is, to:

a. intentionally access computers without authorization, and thereby obtain 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 and information valued at greater than $5,000, in violation of Title 18, United States Code, Section 1030(a)(2)(B) and (C) and 1030(c)(2)(B)(i) and (iii); and

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

MANNERS AND MEANS

12. Members of the conspiracy supported one another, and aided and abetted computer hacking committed by each other, by providing monetary and other incentives, shared computer hacking infrastructure, command and control servers, malware, platforms, tactics, techniques, and procedures for successfully committing unauthorized computer intrusions and stealing victim data.

13. Members of the conspiracy used multiple and evolving sets of sophisticated malware, including publicly-available malware as well as malware uniquely created by the conspirators, in order to obtain, expand, and maintain unauthorized access to protected

computers and related networks. Some of the malware employed by the conspirators included those identified by security researchers as BADFLICK, aka GreenCrash; PHOTO, aka Derusbi; MURKYTOP, aka mt.exe; and HOMEFRY, aka dp.dll. Such malware allowed for initial and continued intrusions into victim systems, lateral movement within a system, and theft of credentials, including passwords.

14. Members of the conspiracy sent fraudulent spear-phishing emails, which appeared to originate from legitimate accounts with a legitimate or innocuous message, but which actually attached malware that would damage and facilitate unauthorized access into the recipient's computer system. The conspirators created online legends, such as fictitious online profiles, for the spear-phishing email accounts in order to further buttress the legitimate appearance of the emails. The conspirators also used doppelganger domain names, which were created to mimic or resemble the domains of legitimate companies, with the intent of tricking unwitting users into clicking on links, as well as hindering identification of intrusions by victim entities.

15. Members of the conspiracy obtained, expanded, and maintained their unauthorized access by stealing means of identification and access devices, including login credentials, belonging to individuals who had administrative access to victim computer systems. In addition, the conspirators used these hijacked credentials, and the access they provided, to launch spear-phishing campaigns against other users of the same system or other victim systems.

16. Members of the conspiracy registered and used malicious and deceptive web domains to store malware until it was used on a particular system, to send spear-phishing emails to intended victims, to store data stolen from victim systems, and as command and control domains for the purpose of controlling malware.

17. Members of the conspiracy used GitHub to store both JavaScript beaconing malware and stolen data. To conceal stolen data stored at GitHub accounts, members of the conspiracy used steganography, which is the concealment of a file within another file, message, video, or picture. Members of the conspiracy also used Application Programming

Interface ("API") keys for Dropbox accounts in commands to upload stolen data directly to Dropbox accounts controlled by the conspirators in order to make it appear that the activity was a legitimate use of the Dropbox service.

18. Members of the conspiracy attempted to obscure their computer hacking activities and theft of data through the use of Internet Protocol anonymizer services, such as The Onion Router ("TOR"). To that end, the conspirators used these services to access DERUSBI and other server-side malware, but also to access their malware infrastructure, including domains and email accounts used in furtherance of their criminal activity. When the private-sector cybersecurity community publicized Hainain Xiandun's hacking efforts, members of the conspiracy observed such efforts and sought to modify their tactics accordingly.

19. Starting as early as 2011, members of the conspiracy coordinated with staff and professors at a university in Hainan ("PRC University 1") to help manage Hainan Xiandun as a front company for the HSSD, to include using the address of PRC University 1's library as an address for Hainan Xiandun; and work with Professor G.J., a computer science professor at PRC University 1, to manage Hainan Xiandun, including the front company's payroll, employee benefits, and recruitment of computer hackers.

20. Despite efforts to conceal HSSD's control over Hainan Xiandun's computer hacking and economic espionage activities, defendants DING XIAOYANG, CHENG QINGMIN, and ZHU YUNMIN maintained and exercised managerial control over Hainan Xiandun, including: (i) corporate formalities and documentation; (ii) payroll issues; (iii) hacking training; (iv) paid vacations; (v) MSS performance awards; and (vi) malware development and vulnerability evaluation for use against foreign governments, companies, and universities

21. Members of the conspiracy also coordinated with staff and professors at PRC University 1 and another College of Technology in Hainan ("PRC College 1"), to identify and recruit talented computer hackers to penetrate foreign entities (including foreign universities) and steal trade secrets, proprietary research, and data, and to identify and

recruit talented linguists to interpret the stolen material. Specifically, between 2012 and 2016, members of the conspiracy:

a. Coordinated, in part with Professor G.J. and Professor L.J., a computer science professor at PRC College 1, on the recruitment of hackers from PRC University 1's College of Software Technology and School of Information as well as PRC College 1, and linguists from the School of Foreign Languages at PRC University 1;

b. Surreptitiously coordinated with PRC University 1 and Professor G.J. to organize and sponsor hacking competitions with monetary prizes, with the goal of identifying hackers for recruitment to Hainan Xiandun.

OVERT ACTS

22. In furtherance of the conspiracy and to effect the objects thereof, the following overt acts, among others, were committed within the Southern District of California and elsewhere:

(1) In or about 2009, defendant DING XIAOYANG joined the MSS, and subsequently began working with the HSSD.

(2) In or about June 2009, defendant ZHU YUNMIN moved from Beijing to Hainan province to join the HSSD.

(3) In or about July 2009, the HSSD established Hainan Kehua ("海南科华") as a front company to recruit computer hackers and linguists to target foreign governments, companies, and universities on behalf of the PRC, similar to Hainan Xiandun ("海南仙盾").

(4) On or about July 8, 2010, defendant ZHU YUNMIN maintained a collection of open source documents regarding leadership and funding for the United States Centers for Disease Control and Prevention, some of which had been translated into Chinese.

(5) From in or about 2010, through at least 2012, defendant CHENG QINGMIN oversaw Hainan Kehua's recruitment of computer hackers,

including from PRC College 1, to engage in computer hacking on behalf of the PRC.

(6) On or about October 17, 2010, defendant ZHU YUNMIN maintained a collection of open source information related to the United States Department of State's Biosecurity Engagement Program.

(7) On or about February 27, 2011, defendant ZHU YUNMIN sought the assistance of a former university classmate in identifying hackers or people who were good at network attacks, and provided salary and other benefits available to those who would engage in such work on behalf of the PRC government.

(8) In or about June 2011, the HSSD established Hainan Xiandun as a front company to recruit computer hackers and linguists to target foreign governments, companies, and universities on behalf of the PRC.

(9) In or about June 2011, members of the conspiracy listed the address for Hainan Xiandun as that of PRC University 1's library and worked with Professor G.J., a PRC University 1 computer science professor, to manage the front company.

(10) On or about June 14, 2011, defendant DING XIAOYANG registered DOMAIN 1, which was to be used as a call-back domain to facilitate computer hacking of multiple entities, including Company A.

(11) On or about June 15, 2011, defendant DING XIAOYANG registered DOMAIN 2, which was to be used as a call-back domain to facilitate computer hacking of multiple entities, including University A, Research Facility A, and NIH.

(12) On or about June 16, 2011, defendant DING XIAOYANG registered DOMAIN 3, which was to be used as a call-back domain to facilitate computer hacking of multiple entities, including University A and NIH.

(13) From in or about 2012, through at least 2017, defendant DING XIAOYANG maintained contact with research institutes within a PRC state-owned shipbuilding corporation, which are responsible for the design of conventional and nuclear-powered submarines.

(14) On or about May 5, 2012, DING XIAOYANG, CHENG QINGMIN, and others received malware from the MSS to be used against foreign victims.

(15) On or about May 10, 2012, members of the conspiracy compiled Gh0stRAT malware, a remote access Trojan, which beaconed to DOMAIN 2, and was used to infiltrate a professor's network account at University A.

(16) On or about August 1, 2012, members of the conspiracy compiled malware, which beaconed to DOMAIN 3, and installed that malware on a system operated by University A no later than November 5, 2012.

(17) On or about August 6, 2012, members of the conspiracy registered DOMAIN 4, which was to be used as a call-back domain to facilitate computer hacking of multiple entities, including University A, Research Facility A, and NIH.

(18) On or about September 11, 2012, members of the conspiracy compiled malware, which beaconed to DOMAIN 2, and was installed on a system operated by University A the following day.

(19) On or about September 11, 2012, members of the conspiracy compiled malware, which beaconed to DOMAIN 4, and was installed on a system operated by University A's School of Medicine.

(20) On or about September 11, 2012, members of the conspiracy compiled malware, which beaconed to DOMAIN 2, to be used to infiltrate computer systems operated by University A's center involved in hydroacoustic and marine research, as well as Research Facility A's program that had begun publicly highlighting its research aimed at a treatment and vaccine for Ebola.

(21) On or about November 1, 2012, members of the conspiracy installed malware, which beaconed to DOMAIN 2, on a system operated by Research Facility A's program that had begun publicly highlighting its research aimed at a treatment and vaccine for Ebola.

(22) In or about November 2012, defendant CHENG QINGMIN coordinated with Professor L.J., a computer science professor at the PRC College 1, to recruit individuals to work for a HSSD front company and engage in computer hacking on behalf of the PRC Government.

(23) In or about January 2013, defendant CHENG QINGMIN oversaw recruitment of computer hackers for Hainan Kehua.

(24) On or about January 8, 2013, members of the conspiracy installed malware, which beaconed to DOMAIN 4, on a system operated by Research Facility A.

(25) On or about January 8, 2013, members of the conspiracy compiled malware, which beaconed to DOMAIN 1, and installed that malware on systems operated by Company A the following day.

(26) On or before January 8, 2013, members of the conspiracy installed malware on a system operated by NIH, which beaconed to DOMAINS 4 and 5.

(27) On or before January 10, 2013, after infiltrating systems operated by NIH, members of the conspiracy conducted multiple term searches on the victim's network, which included "[Research Facility A]," the NIH Office of Biodefense Research Affairs, and possible remote or VPN access to networks.

(28) In or about March 2013, through June 2013, defendant ZHU YUNMIN engaged in the hiring and vetting process on behalf of Hainan Xiandun, including the hiring of defendant WU SHURONG to engage in computer hacking on behalf of the PRC.

(29) On or about March 7, 2013, defendant WU SHURONG applied to join Hainan Xiandun, and was subsequently hired to engage in computer hacking.

(30) In or about May 2013, defendant CHENG QINGMIN oversaw recruitment of computer hackers from PRC University 1's School of Information for a HSSD front company engaged in computer hacking on behalf of the PRC.

(31) On or about May 6, 2013, members of the conspiracy compiled PHOTO malware, a remote access Trojan, accessible with the password "goodperson," and later installed that malware on a system operated by Company A.

(32) From on or about August 4, 2013, through August 28, 2013, members of the conspiracy accessed malware installed at NIH utilizing an IP address that was also utilized to control DOMAIN 4, which members also utilized as a call-back domain for malware.

(33) From on or about September 12, 2013, and through September 16, 2013, members of the conspiracy surreptitiously coordinated with PRC University 1 to sponsor and organize the preliminary rounds of a competition, whose goal was to identify and recruit computer hackers to work on behalf of the MSS.

(34) From on or about October 19, 2013, and through October 20, 2013, members of the conspiracy surreptitiously coordinated with PRC University 1 to organize the final rounds and provide a monetary prize for the winner of a competition, with the goal to identify and recruit computer hackers to work on behalf of the MSS.

(35) From on or about January 1, 2014, through August 6, 2014, members of the conspiracy accessed PHOTO malware with the password "goodperson" on a system operated by Company A, downloaded and ran MURKYTOP, and stole user passwords in order to gain further access to Company A's system.

(36) In or about February 2014, defendant DING XIAOYANG coordinated with PRC University 1 Professor G.J. regarding employment benefits for multiple Hainan Xiandun employees.

(37) On or about February 21, 2014, while at HSSD's headquarters (depicted below), defendant DING XIAOYANG confirmed with PRC University 1 Professor G.J. that payroll and social benefits were paid.



(38) From on or about February 8, 2014, through March 7, 2014, members of the conspiracy accessed malware installed at NIH utilizing an IP address that was also utilized to control DOMAIN 4, a call-back domain for malware used during this same period.

(39) In or about March 2014, defendant DING XIAOYANG oversaw recruitment of English linguists, including from PRC University 1's School of Foreign Languages, to translate computer data and research stolen by computer hackers at Hainan Xiandun.

(40) From on or about March 10, 2014, through April 4, 2014, members of the conspiracy accessed malware installed at a NIH utilizing an IP address that was also utilized to control DOMAIN 4, a call-back domain for malware used during this same period.

(41) On or about April 17, 2014, members of the conspiracy installed malware, which beaconed to DOMAIN 4, on a system operated by Research Facility A.

(42) From on or about May 5, 2014, through May 15, 2014, members of the conspiracy accessed malware installed at NIH utilizing an IP address, to which a subdomain of DOMAIN 4 resolved during this same period.

(43) From on or about July 6, 2014, through August 6, 2014, members of the conspiracy utilized certain IP addresses to access PHOTO malware on a network at Company A, which were also used to access and modify DOMAIN 4, a call-back domain utilized by the members of the conspiracy for malware installed on networks at multiple victims, including University A, Research Facility A, and NIH.

(44) On or about July 25, 2014, members of the conspiracy compiled and installed malware, which beaconed to DOMAIN 4, on a system operated by Research Facility A, which was working on treatments and vaccines for Ebola, which would have been of interest and benefit to multiple Chinese biopharmaceutical companies working on the same topics.

(45) On or about December 29, 2014, members of the conspiracy sent spear phishing emails to four University B employees associated with a robotics engineering program in an attempt to breach its system.

(46) On or about January 8, 2015, through July 1, 2015, members of the conspiracy sought further information about tularemia, Marburg vaccine, Ebola, the U.S. national health security and HIV/AIDS strategies.

(47) On or about January 8, 2015, members of the conspiracy installed MURKYTOP malware on a system operated by University B in order to facilitate lateral movement within that network for the purpose of stealing trade secrets related to autonomous vehicles.

(48) On or about February 21, 2015, members of the conspiracy installed PHOTO malware on a system operated by Research Facility A.

(49) On or about March 25, 2015, members of the conspiracy compiled BADFLICK malware, which beaconed to DOMAIN 4 and was intended to be used to infiltrate a system operated by Research Facility A.

(50) On or about April 20, 2015, members of the conspiracy compiled BADFLICK malware, which was installed on a system operated by Company B on August 5, 2016.

(51) On or about September 16, 2015, members of the conspiracy installed malware on a system operated by University A's center involved in hydroacoustic and marine research.

(52) On or about October 23, 2015, approximately one month after China's President committed to the United States that its government would not conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to the PRC's companies or commercial sectors, members of the conspiracy installed PHOTO malware on a system operated by Company E and later stole proprietary data related to fire-suppression systems and other data.

(53) In or about November 2015, defendant CHENG QINGMIN oversaw recruitment of computer hackers for a HSSD front company.

(54) From on or about December 9, 2015, through January 18, 2016, members of the conspiracy accessed and read internal emails from University B utilizing a web shell accessed by an IP address that was also used to register EMAIL ACCOUNT 2 for a spear phishing campaign.

(55) From on or about December 21, 2015, through January 11, 2016, members of the conspiracy used EMAIL ACCOUNT 2 to send spear phishing emails with embedded malware to multiple defense contractors and

companies specializing in maritime research and development based in the United States, United Kingdom, South Africa, and Austria.

(56) On or about April 11, 2016, members of the conspiracy sought further information related to Ebola.

(57) From on or about July 19, 2016, through August 4, 2016, members of the conspiracy utilized EMAIL ACCOUNT 3 to send spear phishing emails with embedded malware to defense contractors and companies specializing in maritime research and development based in the United States, United Kingdom, and South Africa.

(58) On or about August 4, 2016, members of the conspiracy sent a spear phishing email from EMAIL ACCOUNT 3 to Company B, which breached its system and allowed the defendants to install MURKYTOP malware, a lateral movement tool, and BADFLICK malware in the same network folder, and the MURKYTOP malware was identical to that found on a system operated by Company C.

(59) On or about August 16, 2016, members of the conspiracy installed BADFLICK malware on a system operated by University B.

(60) From on or about August 30, 2016, through August 31, 2016, members of the conspiracy sought further information regarding Company D and "Dropbox appkey," which was a reference to Dropbox API keys.

(61) From on or about August 31, 2016, through November 17, 2016, members of the conspiracy stole approximately 900 files of specialty chemical formulas from Company D, copied them to a Dropbox account, and protected the files with the password "goodperson."

(62) On or about September 2, 2016, on a system operated by Company E, members of the conspiracy installed HOMEFRY malware, a password dumper/cracker, which was identical to that subsequently publicized by a cybersecurity company.

(63) On or about September 24, 2016, members of the conspiracy surreptitiously coordinated with PRC University 1 to sponsor and organize the preliminary round of a competition whose goal was to identify and recruit computer hackers to work on behalf of the MSS.

(64) On or about September 28, 2016, members of the conspiracy copied hundreds of internal documents and video files belonging to Company B to a folder on its network in order to steal that data.

(65) On or about October 29, 2016, members of the conspiracy surreptitiously coordinated with PRC University 1 to organize the final round and provide a monetary prize for the winner of a competition whose goal was to identify and recruit computer hackers to work on behalf of the MSS.

(66) On or about February 10, 2017, members of the conspiracy registered EMAIL ACCOUNT 4, to be used for a spear phishing campaign against the Governments of Cambodia and Saudi Arabia.

(67) In or before March 2017, members of the conspiracy utilized BADFLICK malware to facilitate the installation of HOMEFRY and MURKYTOP malware on a system operated by Company F.

(68) In or before March 2017, members of the conspiracy installed malware on a server that managed Company F's computer system used for communication between flight crews and ground operations in order to ensure uninterrupted access to the airline's network.

(69) On or about March 28, 2017, members of the conspiracy installed BADFLICK malware on a system operated by Research Facility A.

(70) On or about April 9, 2017, members of the conspiracy registered DOMAIN 6, which was to be used as a call-back domain to facilitate computer hacking of multiple entities, including University A, Company C, and Cambodian Government Ministry A, as well as to store malware and stolen data.

(71) On or about April 16, 2017, members of the conspiracy installed malware on a system operated by University A's center involved in hydroacoustic and marine research, which was identical to that stored at DOMAIN 6.

(72) On or about April 19, 2017, members of the conspiracy registered EMAIL ACCOUNT 5 to use for a spear phishing campaign against foreign companies and universities.

(73) On or about May 12, 2017, members of the conspiracy installed MURKYTOP malware on a system operated by University A's center involved in hydroacoustic and marine research.

(74) On or about May 16, 2017, members of the conspiracy installed BADFLICK malware on a system operated by Research Facility A.

(75) On or about June 8, 2017, members of the conspiracy utilized EMAIL ACCOUNT 4 to send spear phishing emails with embedded malware to Cambodian Government Ministry A.

(76) On or about June 13, 2017, members of the conspiracy created a fraudulent LinkedIn account with the same name as EMAIL ACCOUNT 4, where the purported account holder appeared to have been educated in Saudi Arabia, in order to facilitate a spear phishing campaign against the Government of Saudi Arabia.

(77) On or about June 12, 2017, and continuing through June 19, 2017, members of the conspiracy utilized EMAIL ACCOUNT 4 to send spear phishing emails containing malware to Saudi Arabian Government Ministries A and B.

(78) On or about June 13, 2017, members of the conspiracy installed BADFLICK malware on a system operated by Research Facility A.

(79) On or about June 17, 2017, members of the conspiracy installed MURKYTOP malware , which was identical to that stored at DOMAIN 6 and

was subsequently publicized by a cybersecurity company, on a system operated by Research Facility A.

(80) On or about June 21, 2017, members of the conspiracy installed HOMEFRY malware on a system operated by University A's center involved in hydroacoustic and marine research, which was identical to that subsequently publicized by a cybersecurity company.

(81) On or about June 21, 2017, members of the conspiracy installed MURKYTOP malware, which was identical to that stored at DOMAIN 6 and was subsequently publicized by a cybersecurity company, on a system operated by Research Facility A, and executed this malware the following day.

(82) On or about June 21, 2017, members of the conspiracy stole proprietary hydroacoustic research data from University A's center involved in hydroacoustic and marine research utilizing malware installed on its system, which was identical to malware stored at DOMAIN 6, and subsequently publicized by a cybersecurity company.

(83) On or about July 3, 2017, members of the conspiracy utilized BADFLICK malware to assist in executing MURKYTOP malware on a system operated by Research Facility A.

(84) From on or about July 28, 2017, through August 2, 2017, members of the conspiracy utilized two compromised email accounts at Company G to send spear phishing emails to employees of multiple companies, including Company H, which directed recipients to DOMAIN 7, a doppelganger domain impersonating a legitimate Company G domain, that would result in malware being installed on a recipient's computer.

(85) In or about August 2017, defendant CHENG QINGMIN exercised managerial control over Hainan Xiandun, including overseeing training for

Hainan Xiandun technical employees at one of its offices on the 19th floor of Chengtian Garden Building B pictured below.



(86) On or about August 31, 2017, members of the conspiracy installed two pieces of malware on a system operated by University A's center involved in hydroacoustic and marine research, which were identical to malware saved at DOMAIN 6.

(87) On or about September 16, 2017, members of the conspiracy utilized the compromised email account of University C's Director of Applied Research Laboratory to send spear phishing emails to other employees at the same institution, University D's Applied Research Laboratory, University E's Applied Physics Laboratory, University F's Applied Research Laboratory, and University G's Applied Physics Laboratory.

(88) On or about September 20, 2017, members of the conspiracy exfiltrated stolen data from Company E, which included contact information for individuals associated with the controlling authorities for two East-coast ports as well as proprietary data related to fire-suppression systems.

(89) From on or about October 16, 2017, through October 24, 2017, members of the conspiracy stored malware at DOMAIN 6, which was later used to infiltrate University A's computer network, and subsequently publicized by a cybersecurity company.

(90) On or about October 18, 2017, through December 8, 2017, members of the conspiracy utilized EMAIL ACCOUNT 5 to send spear phishing emails containing malware to foreign companies and universities, including University G's Applied Physics Laboratory and University D's Applied Research Laboratory.

(91) On or about October 20, 2017, members of the conspiracy installed MURKYTOP malware on a system operated by Company C as well was an additional piece of malware that was identical to that installed on a system operated by Company B.

(92) On or about October 25, 2017, members of the conspiracy installed MURKYTOP malware on a system operated by University A's center involved with hydroacoustic and marine research, which was identical to the same malware stored at DOMAIN 6.

(93) On or about October 25, 2017, members of the conspiracy installed malware on a system operated by Company H, which was accessed with the password "fuck[Company H]."

(94) On or about October 25, 2017, members of the conspiracy installed malware on a system operated by Company C that beaconed to DOMAIN 6, a call-back domain used by the defendants to control malware.

(95) On or about November 3, 2017, members of the conspiracy installed MURKYTOP malware on a system operated by Company E, which was identical to malware installed on a system operated by Malaysian Political Party A.

(96) On or about November 3, 2017, members of the conspiracy installed PHOTO malware on a system operated by Company H, which was accessible with the password "goodperson" and was identical to PHOTO malware installed on a system operated by University A.

(97) On or about November 3, 2017, members of the conspiracy installed BADFLICK malware on a system operated by Company H, which beaconed to an IP address utilized by DOMAIN 8 during this same time period.

(98) From on or about November 7, 2016, through December 7, 2017, members of the conspiracy utilized EMAIL ACCOUNT 1 to send spear phishing emails embedded with malware to a United States company specializing in maritime research and development, an Indonesian transportation company, University G's Applied Physics Laboratory, and Cambodian Government Ministry A.

(99) On or about November 20, 2017, members of the conspiracy utilized malware to locate and exfiltrate proprietary research data and trade secrets from a system operated by Company H pertaining to U.S. Navy submarine systems development and submarine-launched intercontinental ballistic missiles.

(100) On or about November 22, 2017, members of the conspiracy utilized EMAIL ACCOUNT 6 to send spear phishing emails containing malware to multiple United States defense contractors, and companies specializing in maritime research and development as well as virus and vaccine research and development.

(101) On or about December 5, 2017, members of the conspiracy stored malware at DOMAIN 6, which was later used to infiltrate University A's computer network, and subsequently publicized by a cybersecurity company.

(102) On or about December 6, 2017, members of the conspiracy utilized malware to steal data from a system operated by Malaysian Rail Corporation

A, from whom the China Railway Engineering Group was seeking a multi-billion dollar contract to build a high-speed railway in Malaysia.

(103) On or about December 6, 2017, members of the conspiracy used the email account of a University A professor, which had previously been compromised, to send spear phishing emails containing malware to 32 recipients, including Company C.

(104) On or about December 6, 2017, members of the conspiracy utilized EMAIL ACCOUNT 6 to send test spear phishing emails containing embedded malware and the subject line: "Ocean Physical Story" to EMAIL ACCOUNTS 1 and 5.

(105) On or about December 6, 2017, members of the conspiracy utilized EMAIL ACCOUNT 6 to send spear phishing emails containing embedded malware and the subject line: "Ocean Physical Story" to foreign companies and universities, including University G's Applied Physics Laboratory and University D's Applied Research Laboratory, and intrusion artifacts revealed their specific interest in nanopore data used in virus research that University G had exclusively licensed to a private company.

(106) From on or about December 6, 2017, through December 15, 2017, members of the conspiracy used IP address anonymizing technology in an attempt to conceal control of malware the defendants and their conspirators had installed on a system belonging to University C.

(107) On or about November 3, 2017, members of the conspiracy installed malware on a system operated by Company H, which beaconed to DOMAIN 8.

(108) On or about December 7, 2017, members of the conspiracy registered EMAIL ACCOUNT 7 to send spear phishing emails to Company C and University C.

(109) On or about December 7, 2017, members of the conspiracy registered a Dropbox account to be used to store malware, facilitate intrusions into foreign networks, and act as a depository for proprietary data and trade secrets stolen from foreign companies and universities.

(110) On or about December 13, 2017, members of the conspiracy utilized malware to steal data from a system operated by Malaysian Political Party A, at a time when the party would have played a role in deciding a PRC state-owned enterprise's bid on a railway contract in Malaysia.

(111) On or about December 15, 2017, members of the conspiracy installed malware on a system operated by Company C.

(112) On or about December 28, 2017, members of the conspiracy installed malware on a system operated by Company C that beaconed to DOMAIN 8, a call-back domain used by the defendants to also control malware on a system operated by Company H.

(113) In or before January 2018, members of the conspiracy infiltrated the network of Cambodian Government Ministry A and stole data pertaining to discussions between the Governments of China and Cambodia over use of the Mekong River.

(114) In or about January 2018, members of the conspiracy recruited Cambodian linguists to translate stolen data stolen from the Cambodian Government, which they protected with the password "goodperson" and stored at DOMAIN 6, a call-back domain for malware used by the defendants.

(115) On or about January 7, 2018, members of the conspiracy stored malware at DOMAIN 6, which was later used to infiltrate University A's computer network and was identical to malware subsequently publicized by a cybersecurity company.

(116) On or about January 10, 2018, the same day that the PRC was engaged in discussions with multiple countries, including Cambodia, concerning use

of the Mekong River, members of the conspiracy stole data from a system operated by Cambodian Government Ministry A pertaining those discussions, and stored that data at DOMAIN 6, where it was protected with the password "goodperson."

(117) On or about January 10, 2018, members of the conspiracy stored malware in a GitHub account that had been specifically created for intrusions at Company C and University C, as well as other foreign companies.

(118) On or about January 10, 2018, members of the conspiracy sent stolen trade secrets and proprietary hydroacoustic data to a GitHub account using the following steganographs of a koala bear and President Donald Trump.





(119) On or about January 19, 2018, members of the conspiracy sent stolen trade secrets and proprietary hydroacoustic data to a GitHub account using a stegonograph of President Donald Trump.

(120) On or about March 6, 2018, members of the conspiracy installed MURKYTOP malware on a system operated by University A's center involved in hydroacoustic and marine research, which was identical to that stored at DOMAIN 6 and was subsequently publicized by a cybersecurity company.

(121) On or about March 9, 2018, members of the conspiracy installed multiple pieces of malware on a system operated by University A's center

involved in hydroacoustic and marine research, including PHOTO malware, which was accessible with the password "goodperson."

(122) On or about May 29, 2018, defendant DING XIAOYANG was presented an award from the MSS for young leaders in the organization while he was overseeing computer hacking and theft of data conducted by Hainan Xiandun, as depicted in the following photograph:



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

Count 2

Conspiracy to Commit Economic Espionage

23. The allegations contained in paragraphs 1 through 22, including Overt Acts 1-122, are realleged and incorporated as if set forth herein.

24. Beginning on a date unknown, and continuing through on or about September 2018, within the Southern District of California and elsewhere, defendants DING XIAOYANG, aka Ding Hao, aka Manager Chen, CHENG QINGMIN, aka Manager Cheng, and ZHU YUNMIN, aka Zhu Rong, and WU SHURONG, aka goodperson, aka ha0r3n, aka Shi Lei, did, without authorization, knowingly and intentionally conspired with each other,

and others known and unknown to the Grand Jury, with the knowledge and intent of benefitting a foreign government, to wit, the PRC, to:

a. Steal, and without authorization appropriate, take, carry away, and conceal, by fraud artifice, and deception obtain a trade secret;

b. Without authorization copy, duplicate, sketch, draw, photograph, download, upload, alter, destroy, photocopy, replicate, transmit, deliver, send, mail, communicate, and convey a trade secret; and

c. Receive, buy, and possess a trade secret, knowing the same to have been stolen or appropriated, obtained, and converted without authorization.

25. DING XIAOYANG, CHENG QINGMIN, ZHU YUNMIN, and WU SHURONG conspired to steal trade secret information from University B, University G, and Company H. Each of the victims took reasonable measures to keep this information secret, and such information derived independent economic value from not being generally known, and not being readily ascertainable through proper means by another person.

26. In furtherance of the conspiracy, and to effect the purpose and objectives thereof, defendants DING XIAOYANG, CHENG QINGMIN, ZHU YUNMIN, and WU SHURONG, and others, committed various overt acts in the Southern District of California and elsewhere, including, but not limited to, the overt acts identified in paragraphs 50, 58, 64, 84, 87, 90-91, 93, 96-99, 105, 107, and 112, in violation of Title 18, United States Code, Section 1831(1-3); all in violation of Title 18, United States Code, Section 1831(5).

Criminal Forfeiture

27. Upon conviction of the offenses alleged in this indictment, defendants DING XIAOYANG, aka Ding Hao, aka Manager Chen, CHENG QINGMIN, aka Manager Cheng, ZHU YUNMIN, aka Zhu Rong, and WU SHURONG, aka goodperson, aka ha0r3n, aka Shi Lei, shall forfeit to the United States of America, pursuant to Title 18, United States Code, Section 982(a)(1), any property, real and personal, involved in such offenses, and any property traceable to such property.

28. In the event that any of the property described above, 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 which cannot be divided without difficulty,

the United States of America shall be entitled to forfeit substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b)(1).

All in violation of Title 18, United States Code, Section 982(a)(1) and (b)(1).

DATED: May 28, 2021.

A TRUE BILL:

Foreperson

RANDY S. GROSSMAN
Acting United States Attorney

By:
FRED SHEPPARD
Assistant U.S. Attorney

I hereby attest and certify on May 28, 2021 that the foregoing document is a full, true and correct copy of the original on file in my office and in my legal custody.

Clerk, U.S. District Court
Southern District of California

By: s/ E. Blase
Deputy