CRH:DMP/SK/JKW
F. #2017R00077

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X

UNITED STATES OF AMERICA

- against -

NI GAOBIN (倪高彬),
WENG MING (翁明),
CHENG FENG (程锋),
PENG YAOWEN (彭耀文),
SUN XIAOHUI (孙小辉),
XIONG WANG (熊旺) and
ZHAO GUANGZONG (赵光宗),

Defendants.

----------X

I N D I C T M E N T

Cr. No. 24-CR-43
(T. 18, U.S.C., §§ 371, 981(a)(1)(C), 982(a)(2), 982(b)(1), 1030(i)(1), 1030(i)(2), 1349 and 3551 et seq.; T. 21, U.S.C., § 853(p); T. 28, U.S.C., § 2461(c))

Judge Ramon E. Reyes
Magistrate Judge Peggy Kuo

THE GRAND JURY CHARGES:

INTRODUCTION

At all times relevant to this Indictment, unless otherwise stated:

I. Overview of Chinese Intelligence Services' Structure and Activities

1. The People's Republic of China ("PRC") conducted intelligence activities using a variety of sources, including through the Ministry of State Security ("MSS"). The MSS was the foreign intelligence and police agency of the PRC, handled civilian intelligence collection for the PRC and was responsible for the PRC government's counterintelligence, espionage and political security functions. The MSS consisted of a central ministry, provincial state security departments based in each of the PRC's provinces and municipal state security bureaus.

2. The MSS and its state security departments sought to obtain information on political, economic and security policies that might affect the PRC, along with military, scientific and technical information of value to the PRC. Among other things, the MSS and its state security departments focused on surreptitiously identifying and influencing the foreign policy of other countries, including the United States. In many instances, the MSS focused collection and subsequent related malign influence efforts on politicians that the PRC perceived as being critical of PRC government policies. The MSS also sought to target intellectual property that could be utilized to the economic advantage of PRC-based commercial firms.

3. One of the ways the MSS collected information was through computer intrusion activity, of which individuals and entities in the United States were a principal target.

4. The Hubei State Security Department ("HSSD") was the provincial foreign intelligence arm of the MSS in Hubei Province, PRC. The HSSD was located on Bayi Road, Wuchang District, in Wuhan, a city in Hubei Province.

5. In approximately 2010, the HSSD created a front company, Wuhan Xiaoruizhi Science & Technology Co., Ltd. (武汉晓睿智科技有限责任公司) ("Wuhan XRZ"), to carry out its computer intrusion activities. A PRC government business license issued by the PRC Administration for Market Regulation described Wuhan XRZ as a company involved with research and experimental development, technology development, technology consultation and technology transfer.

II. The Defendants

6. The defendant NI GAOBIN (倪高彬) is a 38-year-old citizen of the PRC. NI conducted hacking activities in support of the MSS's foreign intelligence and economic

espionage objectives, as well as targeting Hong Kong democracy activists and members of the Uyghur minority group. A photograph of NI is depicted below:

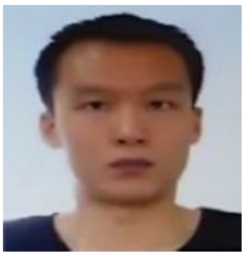
7. The defendant WENG MING (翁明) is a 37-year-old citizen of the PRC. WENG conducted hacking activities in support of the MSS's foreign intelligence and economic espionage objectives. A photograph of WENG is depicted below:

8. The defendant CHENG FENG (程锋) is a 34-year-old citizen of the PRC. CHENG engaged in hacking activities as a contractor for HSSD's front company, Wuhan XRZ, in support of the MSS's foreign intelligence and economic espionage objectives. A photograph of CHENG is depicted below:

9. The defendant PENG YAOWEN (彭耀文) is a 38-year-old citizen of the PRC. PENG engaged in hacking activities as a contractor for HSSD's front company, Wuhan XRZ, in support of the MSS's foreign intelligence and economic espionage objectives. A photograph of PENG is depicted below:

10. The defendant SUN XIAOHUI (孙小辉) is a 38-year-old citizen of the PRC. SUN was the owner of Wuhan Liuhe Tiangong Science & Technology Co., Ltd. ("Wuhan Liuhe"), a private company, and engaged in hacking activities in support of the MSS's foreign intelligence and economic espionage objectives. A photograph of SUN is depicted below:

11. The defendant XIONG WANG (熊旺) is a 34-year-old citizen of the PRC. XIONG engaged in hacking activities as a contractor for HSSD's front company, Wuhan XRZ, in support of the MSS's foreign intelligence and economic espionage objectives. A photograph of XIONG is depicted below.



12. The defendant ZHAO GUANGZONG (赵光宗) is a 38-year-old citizen of the PRC. ZHAO engaged in hacking activities as a contractor for HSSD's front company, Wuhan XRZ, in support of the MSS's foreign intelligence and economic espionage objectives. A photograph of ZHAO is depicted below:

III. The Criminal Scheme

A. Overview

13. From at least 2010 through January 2024, the HSSD was responsible for a wide variety of computer network exploitation and computer intrusion activities, operating in part through the front company Wuhan XRZ and receiving the support of Wuhan Liuhe. This malicious cyber activity resulted in the mass targeting of thousands of U.S. and foreign politicians, foreign policy experts, academics, journalists and democracy activists, as well as persons and companies operating in areas of national importance, including the defense,

information technology ("IT"), telecommunications, manufacturing and trade, finance, consulting, legal and research industries.

14. The defendants NI GAOBIN, WENG MING, CHENG FENG, PENG YAOWEN, SUN XIAOHUI, XIONG WANG and ZHAO GUANGZONG, together with dozens of identified MSS intelligence officers, contractor hackers and support personnel, were part of a group of malicious cyber actors operating on behalf of the HSSD. The group was known by cybersecurity researchers as "Advanced Persistent Threat 31" or "APT 31," "Zirconium," "Violet Typhoon," "Judgment Panda" and "Altaire."

15. Since at least 2010, the defendants NI GAOBIN, WENG MING, CHENG FENG, PENG YAOWEN, SUN XIAOHUI, XIONG WANG and ZHAO GUANGZONG, and others known and unknown (the "Conspirators"), engaged in computer network intrusion activity on behalf of the HSSD targeting numerous U.S. government officials, various U.S. economic and defense industries and a variety of private industry officials, foreign democracy activists, academics and parliamentarians in response to geopolitical events affecting the PRC. These computer network intrusion activities resulted in the confirmed and potential compromise of work and personal email accounts, cloud storage accounts and telephone call records belonging to millions of Americans, including at least some information that could be released in support of malign influence targeting democratic processes and institutions, and economic plans, intellectual property, and trade secrets belonging to American businesses, and contributed to the estimated billions of dollars lost every year as a result of the PRC's state-sponsored apparatus to transfer U.S. technology to the PRC.

B. Targeting of U.S. and Other Government and Political Officials

16. Since at least 2015, the Conspirators sent thousands of malicious tracking email messages to the personal and professional email accounts of government and political officials in the U.S. and elsewhere, including targets' family members and contacts. The malicious email messages generally purported to be from prominent American journalists, contained email subject headers purporting to contain legitimate news articles, and the body of the messages purported to include excerpts from news articles from news outlets, such as CNN and Vox. However, the messages contained an embedded hyperlink that served as a tracking link. If the recipient activated the tracking link by opening the email, information about the recipient, including the recipient's location, IP addresses, network schematics and specific devices used to access the pertinent email accounts, was transmitted to a server controlled by the Conspirators. The Conspirators used this method to enable more direct and sophisticated targeting of recipients' home routers and other electronic devices, including those of high-ranking U.S. government officials and politicians and election campaign staff from both major U.S. political parties.

17. Between approximately June and September 2018, the Conspirators sent more than 10,000 malicious email messages to professional and personal email addresses belonging to high-ranking U.S. government officials and their advisors, including officials involved in international policy and foreign trade issues. The targets included individuals at the White House; the Departments of Justice, Commerce, Treasury and State; members of Congress, including both Democratic and Republican U.S. Senators from more than ten states; government officials in the Eastern District of New York; and the spouses of a high-ranking Department of Justice official, high-ranking White House officials and multiple United States Senators. The

targets also included political strategists and commentators and political and special interest advocates, as well as U.S. government contractors, including cleared defense contractors, to obtain U.S. government information.

18. In or about May 2020, the Conspirators began targeting email accounts belonging to several senior campaign staff members for a presidential campaign. In or about November 2020, the Conspirators sent emails containing tracking links to targets associated with additional political campaigns, including a retired senior U.S. government national security official.

19. In or about March 2022, the Conspirators sent emails containing tracking links to various government officials in the U.S. Senate, the State Department and the Departments of Commerce, Labor and Transportation.

20. In addition to targeting U.S. government and political officials, the Conspirators also targeted other government officials around the world who expressed criticism of the PRC government. For example, in or about 2021, the Conspirators targeted the email accounts of various government individuals from across the world who were part of the Inter-Parliamentary Alliance on China ("IPAC"), a group founded in 2020 on the anniversary of the 1989 Tiananmen Square protests whose stated purpose was to counter the threats posed by the Chinese Communist Party to the international order and democratic principles. In or about January 2021, the Conspirators registered and used ten Conspirator-created accounts on an identified mass email and mail merge system to send more than 1,000 emails to more than 400 unique accounts of individuals associated with IPAC. Similar to the mailing tools utilized to target U.S. officials and politicians, the mailing tool used in this campaign allowed the Conspirators to track delivery metrics on emails and receive data from victims that opened the

emails, including the victims' IP addresses, browser types, and operating systems. The targets included every European Union member of IPAC, and 43 United Kingdom parliamentary accounts, most of whom were members of IPAC or had been outspoken on topics relating to the PRC government.

C. Targeting of U.S. Economic and Defense Industries

21. Between at least 2010 and November 2023, the Conspirators used sophisticated cyber means to hack and attempt to hack into protected computers, that is, computers used in and affecting interstate and foreign commerce and communications, to steal non-public information.

22. To achieve these intrusions, the Conspirators used sophisticated types of custom malware such as RAWDOOR, Trochilus, EvilOSX, DropDoor/DropCat and others. This malware used legitimate executable files to side-load malicious DLL (dynamic link library) files, which decrypted and executed payloads, or implants, on the victim machines. The implants established secure connections with accounts or servers controlled by the Conspirators in order to receive and execute commands on the victim machines. The Conspirators later began using against victim networks a cracked/pirated version of a commercial cybersecurity penetration testing tool called Cobalt Strike Beacon.

23. One such example was the targeting of a U.S. cleared defense contractor with offices in Long Island, New York and elsewhere (the "Defense Contractor"). Between approximately October 2016 and December 2016, the Conspirators used a zero-day privilege escalation exploit—a vulnerability in a computer system that hackers become aware of prior to efforts by a vendor or user of the computer system to patch or fix the vulnerability—to gain access to the Defense Contractor. Using the zero-day privilege escalation exploit, the

Conspirators first obtained administrator access to a subsidiary's network before ultimately pivoting into the Defense Contractor's core corporate network. The Conspirators used a SQL injection, in which they entered malicious code into a web form input box to gain access to information that was not intended to be displayed, to create an account on the subsidiary's network with the username "testdew23." The Conspirators used malicious software to grant administrator privileges to the "testdew23" user account. Next, the Conspirators uploaded a web shell, or a script that enables remote administration of the computer, named "Welcome to Chrome," onto the subsidiary's web server. Thereafter, the Conspirators used the web shell to upload and execute at least two malicious files on the web server, which were configured to open a connection between the victim's network and computers outside that network that were controlled by the Conspirators. Through this method, the Conspirators successfully gained unauthorized access to the Defense Contractor's network.

24. In another example, between approximately 2017 and 2019, the Conspirators targeted and gained access to the networks of seven IT managed service providers, including providers based in New York, California, Massachusetts, Colorado, Idaho and overseas. IT managed service providers were third-party organizations that customers contracted to manage one or more specialized technological needs, such as network management and security. Customers of managed service providers included corporations, non-government organizations and small- and medium-sized businesses. By hacking these networks, the Conspirators gained access to the data belonging to customers of the breached managed service providers. In one such computer intrusion, in approximately May 2017, the Conspirators accessed a backup server belonging to a California-based managed service provider ("California MSP") and, from there, accessed servers belonging to the California MSP's customers. Using

malicious files hidden in network security programs, the Conspirators gained access to at least 35 devices on the California MSP's network and exploited the California MSP's access to customer networks to spread malware to at least 15 servers on as many as seven remote customer networks. The affected California MSP customers included a financial company, a nuclear power engineering company, an enterprise-resources planning company and three additional IT managed service providers.

25. Between at least 2010 and November 2023, the Conspirators also gained access to the following companies, research institutions and other organizations in the following industries, among others:

a. the defense industry, including a cleared defense contractor based in Oklahoma that designed and manufactured military flight simulators for the U.S. Army, Air Force and Navy; a cleared aerospace and defense contractor based in Tennessee; an Alabama-based research corporation in the aerospace and defense industries; and a Maryland-based professional support services company that serviced the Department of Defense and other government agencies;

b. the IT industry, including a leading American manufacturer of software and computer services based in California; a leading global provider of wireless technology based in Illinois; a technology company based in New York; a software company servicing the industrial controls industry based in California; an IT consulting company based in California; an IT services and spatial processing company based in Colorado; a multi-factor authentication company; an American trade association [redacted]; and multiple information technology training and support companies;

c. the telecommunications industry, including a leading provider of 5G network equipment in the United States; an IT solutions and 5G integration service company based in Idaho; a telecommunications company based in Illinois; and a voice technology company headquartered in California;

d. the manufacturing and trade industry, including a prominent trade organization with offices in New York and elsewhere; a manufacturing association based in Washington, D.C.; a steel company based in [redacted]; an apparel company based in New York; an engineering company based in California; and an energy company based in Texas;

e. the finance and consulting industry, including a finance company headquartered in New York; an American multi-national management consulting company with offices in Washington, D.C. and elsewhere; a financial ratings company based in New York; an advertising agency based in New York; and a consulting company based in Virginia;

f. the legal industry, including multiple global law firms based in New York and throughout the United States, and a law firm software provider; and

g. the research industry, including a machine learning laboratory based in Virginia; a university based in California; multiple research hospitals and institutes located in New York and Massachusetts; and an international non-profit organization headquartered in Washington, D.C.

D. Hacking in Response to Geopolitical Events Affecting the PRC

26. Since at least 2017, the Conspirators engaged in computer network intrusion activity in response to geopolitical events affecting the PRC, including economic tensions between the U.S. and the PRC, the Hong Kong democracy movement and a U.S. government statement regarding the PRC's maritime claims in the South China Sea.

i. Hacking in Response to U.S.-PRC Economic Tensions

27. On or about March 8, 2018, amid ongoing economic tensions between the U.S. and the PRC over import duties on products from the PRC, the United States implemented a new tariff on imported steel. In response, the PRC Ministry of Commerce publicly stated that the PRC would "immediately fight back with a major response." Within hours of that announcement, on or about March 9, 2018, the Conspirators registered a malicious domain impersonating the legitimate domain of one of the largest steel producers in the United States (the "American Steel Company"). On or about March 17, 2018, the Conspirators registered malicious domains impersonating the legitimate domain of an international steel trade forum (the "International Steel Trade Forum"). These malicious domains allowed the Conspirators to communicate with malware they installed on the network of the American Steel Company to access and surveil the victim.

ii. Hacking in Response to the Hong Kong Democracy Movement

28. In February 2018, U.S. lawmakers nominated for the Nobel Peace Prize several activists who spearheaded Hong Kong's Umbrella Movement, a 2014 movement in which protestors rallied for political reforms in Hong Kong while using umbrellas to shield themselves from pepper spray that police used to disperse the rallies. The Nobel Peace Prize was to be decided by the Norwegian Nobel Committee, a five-member committee appointed by the Norwegian Parliament. In response to the nomination, the Conspirators targeted the Norwegian government and a Norwegian multinational managed service provider (the "Norwegian MSP") using DropDoor/DropCat malware. The DropDoor/DropCat malware forced the compromised computer to download and process commands that the Conspirators stored in an account on an

online file storage platform and encrypted and uploaded stolen data from the compromised network to that same account.

29. Throughout 2019, in response to continued protests in Hong Kong, the Conspirators conducted widescale hacking activities targeting Hong Kong pro-democracy activists located in the United States and abroad, as well as legislators, activists and journalists associated with the Hong Kong democracy movement. In or about October 2019, the Conspirators created email accounts impersonating prominent PRC dissident activists and used these imitation email accounts to target other critics of the PRC government with malicious emails. The emails contained a link that, if accessed, resulted in DropDoor/DropCat malware being installed on the victims' machines. Through this technique, the Conspirators were able to successfully gain information about PRC government critics.

30. In or about October 2019, the Conspirators targeted Hong Kong legislators with malicious emails. The emails contained a link to a file named "FYI.zip," and the "zipped" archive contained documents that appeared to relate to the Hong Kong protests, including documents titled "Hong-Kong-Report.pdf" and "Hong-Kong-Democratic-Crisis-Brief.pdf." The zip file contained a "shortcut" file designed to download and execute a malicious file—the DropDoor/DropCat malware—that was hosted on an online file storage platform. Also in or about October 2019, the Conspirators used the same technique to successfully target at least seven Hong Kong democracy activists.

iii. Hacking in Response to a U.S. Statement Regarding the PRC's Maritime Claims in the South China Sea

31. On or about July 13, 2020, the United States Secretary of State characterized the PRC's territorial claims in the South China Sea as "completely unlawful." The following day, the U.S. Assistant Secretary of State for East Asian and Pacific Affairs added that

the PRC sought to "replace international law with rule by threats and coercion." The PRC Embassy in Washington, D.C. responded in a statement, asserting that the U.S. Assistant Secretary of State's "accusation is completely unjustified."

32. In or about July 2020, in response to the State Department's allegations concerning the South China Sea, the Conspirators used an Estonian-based email account to send malicious emails to a variety of victims in the United States and Asia, including the U.S. Naval Academy, the U.S. Naval War College's China Maritime Studies Institute and an American think tank focused on U.S. national security issues, including in the Asia-Pacific region.

33. The emails were designed to prompt the recipients to download and execute a file named "macfee" from a shared software repository. The executable file was a malware "dropper" that, if installed, would launch a legitimate McAfee anti-virus application while simultaneously installing and running the DropDoor/DropCat malware implant. The DropDoor/DropCat malware implant was configured with settings previously associated with the October 2019 intrusion activity involving the Hong Kong legislators and democracy activists.

COUNT ONE
(Conspiracy to Commit Computer Intrusions)

34. The allegations contained in paragraphs one through 33 of this Indictment are repeated and realleged as if fully set forth herein.

35. In or about and between December 2014 and January 2024, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants NI GAOBIN (倪高彬), WENG MING (翁明), CHENG FENG (程锋), PENG YAOWEN (彭耀文), SUN XIAOHUI (孙小辉), XIONG WANG (熊旺) and ZHAO GUANGZONG (赵光宗), together with others, did knowingly and willfully conspire to:

(a) intentionally access without authorization one or more computers and thereby to obtain information from one or more protected computers, contrary to Title 18, United States Code, Sections 1030(a)(2)(C), 1030(c)(2)(A) and 1030(c)(2)(B); (b) knowingly cause the transmission of a program, information, code and command, and as a result of such conduct, intentionally cause damage without authorization to a protected computer, contrary to Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B); and (c) intentionally access a protected computer without authorization and as a result of such conduct recklessly cause damage, contrary to Title 18, United States Code, Sections 1030(a)(5)(B) and 1030(c)(4)(A).

36. In furtherance of the conspiracy, and to effect its objects, the defendants NI GAOBIN (倪高彬), WENG MING (翁明), CHENG FENG (程锋), PENG YAOWEN (彭耀文), SUN XIAOHUI (孙小辉), XIONG WANG (熊旺) and ZHAO GUANGZONG (赵光宗), together with others, did commit and cause the commission of the following:

OVERT ACTS

a. In or about December 2014, PENG YAOWEN and SUN XIAOHUI maintained an encrypted target list containing the names of 12 U.S. entities against whom PENG and SUN conducted research and reconnaissance throughout 2014 and 2015 and against whom the Conspirators executed intrusion campaigns between 2014 and at least 2018.

b. In or about 2015, WENG MING sent via email to SUN XIAOHUI a malware variant called Gh0stRAT that the Conspirators used in approximately 2015.

c. In or about February 2015, PENG YAOWEN and SUN XIAOHUI used a web shell to maintain unauthorized network access to a server on a private U.S. university's network.

d. In or about April 2015, PENG YAOWEN and SUN XIAOHUI used a web shell to maintain unauthorized network access to a server on a U.S. engineering company's network.

e. In or about and between 2015 and 2016, CHENG FENG—while employed by Wuhan XRZ and co-located with an identified MSS officer—conducted development work on a malware implant called RAWDOOR, which the Conspirators used regularly from approximately 2015 to 2017 to target victim companies.

f. In or about 2015, CHENG FENG worked to develop a key-logger tool, which permitted the Conspirators to track the activity of the user of a targeted computer by recording the user's keystrokes.

g. In or about 2015, CHENG FENG managed credentials used to register an online account containing unique files that were part of the Conspirators' use of the RAWDOOR malware.

h. In or about 2015, CHENG FENG managed a domain name for a command-and-control server that accessed at least 59 unique victim computers, many of which the Conspirators targeted with the RAWDOOR malware, including a telecommunications company that was a leading provider of 5G network equipment in the United States, an Alabama-based research corporation in the aerospace and defense industries and a Maryland-based professional support services company that serviced the Department of Defense and other government agencies.

i. In or about 2015, CHENG FENG controlled another domain name that spoofed the name of a major U.S. smartphone and technology manufacturer.

j. In or about and between October 2016 and December 2016, the Conspirators conducted intrusion activity against the Defense Contractor.

k. In or about and between October 2017 and 2020, NI GAOBIN conducted extensive computer hacking-related research.

l. In or about and between 2017 and 2018, NI GAOBIN exchanged test emails containing tracking links and malware links with multiple alternate email addresses controlled by NI.

m. In or about and between 2017 and 2018, NI GAOBIN accessed domain registrar accounts and/or virtual private server ("VPS") accounts used to host command-and-control domains used by the Conspirators to conduct intrusion activities.

n. In or about 2018, CHENG FENG, XIONG WANG and ZHAO GUANGZONG possessed and tested a malware variant called EvilOSX that targeted Apple computers. CHENG, XIONG and ZHAO created a malicious web page on a server controlled by the Conspirators that resembled a legitimate download page for the common software product Adobe Flash; however, the "Install now" button was configured to direct the user to a malicious website. As a result, an unsuspecting victim trying to download Adobe Flash instead would download the EvilOSX malware, which, once installed by a victim, was programmed to communicate with a command-and-control domain hosted at a server leased by the Conspirators.

o. In or about 2018, WENG MING and SUN XIAOHUI operated the infrastructure used in an intrusion into a U.S. [redacted] company known for its public opinion polls.

p. In or about 2018, the Conspirators used tracking link emails to target four of the 12 entities on the target list maintained by PENG YAOWEN and SUN XIAOHUI in December 2014.

q. On or about March 9, 2018, the Conspirators registered a domain with a Bulgarian domain registrar impersonating the legitimate domain of the American Steel Company.

r. On or about March 17, 2018, the Conspirators registered with the same Bulgarian domain registrar a second malicious domain which impersonated the legitimate domain of the International Steel Trade Forum.

s. In or about and between March 2018 and May 2018, the Conspirators installed and maintained malware, including a malware implant known as Trochilus, on the network of the American Steel Company, and used a malicious domain purchased through an Australian VPS company and hosted on a server in Los Angeles, California as a command-and-control server through which the Conspirators could direct infected computers and receive stolen data from the American Steel Company.

t. On or about April 26, 2018, the Conspirators temporarily reconfigured the malicious domains associated with the malware for the American Steel Company in response to mitigation steps taken by the victim. As a result of the reconfiguration, the malware ceased communications with the Conspirators' command-and-control server to prevent the victim from discovering a second piece of recovery malware that the Conspirators had installed on the American Steel Company's network as a backup to the Trochilus malware implant.

u. In or about and between April 2018 and September 2018, the Conspirators deployed the DropDoor/DropCat malware into the Norwegian MSP's network. The malware beaconed to an account at an online file storage platform that permitted the Conspirators to control the malware and to receive data that was exfiltrated from the Norwegian MSP. The Conspirators installed the malware used in the Norwegian MSP intrusion through a file named "gup.exe." The Conspirators conducted online research on gup.exe in April 2018, and then in or about July 2018, began accessing the website of the Nobel Prize Committee, including identifying the members who served on the committee.

v. In or about and between June and September 2018, the Conspirators conducted an intrusion into the networks of a manufacturing advocacy group (the "Manufacturing Advocacy Group"), during which the Conspirators targeted three of the group's executives and a board member.

w. In or about and between June 2018 and June 2019, the Conspirators installed DropDoor/DropCat malware on the Manufacturing Advocacy Group's networks.

x. On or about and between June 27, 2018 and June 29, 2018, the Conspirators sent malicious email messages to various State Department employees that purported to originate from the email address "no_reply@insimagecloud.com," used subject lines such as "Why is the United States not at the 2018 World Cup?," and purported to contain excerpts from news articles. The emails had hyperlinks within the purported news excerpts that contained tracking links that beaconed the victims' data to the Conspirators.

y. In or about and between June and July 2018, the Conspirators sent malicious email messages to U.S. government officials, including government officials in the

Eastern District of New York, from at least three different domains, including the domains @usnews-today.com, @insimagecloud.com and @timelynews.us.

z. In or about and between August and September 2018, the Conspirators sent malicious email messages to U.S. government officials from several domains including @dailytrainnews.com, @europeanew.com, @nynewsweek.com and @nytrainnews.com.

aa. In or about and between August and September 2018, the Conspirators sent tracking link emails to personal email accounts of various State Department employees.

bb. In or about and between August and September 2018, the Conspirators sent emails to the spouses of certain U.S. government officials, including the spouses of the Department of Justice leadership, White House officials and multiple United States Senators, seeking to obtain the targets' IP addresses and web browser versions and to gain unauthorized access to the targets' home routers and other electronic devices.

cc. In or about 2019, NI GAOBIN and ZHAO GUANGZONG sent emails with links to files containing malware to Hong Kong legislators and democracy activists.

dd. In or about July 2020, NI GAOBIN and ZHAO GUANGZONG used an Estonian-based email account to send emails with links to files containing malware to victims in the United States and Asia, including the U.S. Naval Academy, the U.S. Naval War College's China Maritime Studies Institute and a U.S. think tank focused on U.S. national security issues, including in the Asia-Pacific region.

ee. In or about August 2020, NI GAOBIN and ZHAO GUANGZONG used an Estonian-based email account to target Hong Kong democracy activists with malware

implants. The emails contained a shortcut designed to download and execute a file from an online hosting platform that hosted four .pdf files that purported to relate to COVID-19 vaccines. Each of these .pdf files were executable "Windows Installer" files containing DropDoor/DropCat malware implants configured to receive commands from an account at an online file sharing platform that was controlled by NI and ZHAO.

ff. In or about May 2020, the Conspirators targeted email accounts belonging to senior campaign staff members for a presidential campaign. The Conspirators sent tracking link emails from an email account that spoofed the name of a prominent American journalist. The subject lines of the emails referred to a news article, and the body of the emails contained a copy of the news article as well as a hidden tracking link hosted at the domain newsinslowusa.com, controlled by the Conspirators.

gg. In or about November 2020, the Conspirators sent emails containing tracking links, purporting to be from a journalist with a major broadcast network and purporting to attach an election-related news article, to targets associated with other political campaigns, including a former senior U.S. government national security official.

hh. In or about and between 2020 and 2021, WENG MING worked with a malware variant based on Cobalt Strike Beacon software that the Conspirators used in approximately 2020 and 2021.

ii. In or about March 2022, the Conspirators sent emails containing tracking links to the personal email accounts of various government officials in the U.S. Senate and the Departments of Commerce, Labor, State and Transportation. These emails purported to be from a producer of another major broadcast network.

jj. In or about June 2022, the Conspirators had compromised and placed under email surveillance three personal accounts belonging to a former U.S. Cabinet official.

kk. In or about and between June 2022 and February 2023, the Conspirators had compromised and placed under email surveillance a personal account belonging to a current United States Ambassador to a Southeast Asian country.

(Title 18, United States Code, Sections 371 and 3551 et seq.)

COUNT TWO
(Wire Fraud Conspiracy)

37. The allegations contained in paragraphs one through 33 and 36 of this Indictment are repeated and realleged as if fully set forth herein.

38. In and about and between December 2014 and January 2024, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants NI GAOBIN (倪高彬), WENG MING (翁明), CHENG FENG (程锋), PENG YAOWEN (彭耀文), SUN XIAOHUI (孙小辉), XIONG WANG (熊旺) and ZHAO GUANGZONG (赵光宗), together with others, did knowingly and intentionally conspire to devise a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, to transmit or cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds, to wit: communications with victim computers to create and maintain unauthorized access to

those computers in order to obtain proprietary and valuable information from them, contrary to Title 18, United States Code, Section 1343.

(Title 18, United States Code, Sections 1349 and 3551 et seq.)

CRIMINAL FORFEITURE ALLEGATION
AS TO COUNT ONE

39. The United States hereby gives notice to the defendants NI GAOBIN (倪高彬), WENG MING (翁明), CHENG FENG (程锋), PENG YAOWEN (彭耀文), SUN XIAOHUI (孙小辉), XIONG WANG (熊旺) and ZHAO GUANGZONG (赵光宗), that, upon their conviction of the offense charged in Count One, the government will seek forfeiture in accordance with Title 18, United States Code, Sections 982(a)(2) and 1030(i)(1), which require any person convicted of such offense to forfeit any property constituting, or derived from, proceeds obtained directly or indirectly as a result of such offense, and such person's interest in any personal property that was used or intended to be used to commit or to facilitate such offense.

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

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third 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;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 982(b)(1) and 1030(i)(2), to seek forfeiture of any other property of the defendants up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Sections 982(a)(2), 982(b)(1), 1030(i)(1) and 1030(i)(2); Title 21, United States Code, Section 853(p))

CRIMINAL FORFEITURE ALLEGATION
AS TO COUNT TWO

41. The United States hereby gives notice to the defendants NI GAOBIN (倪高彬), WENG MING (翁明), CHENG FENG (程锋), PENG YAOWEN (彭耀文), SUN XIAOHUI (孙小辉), XIONG WANG (熊旺) and ZHAO GUANGZONG (赵光宗), that, upon their conviction of the offense charged in Count Two, the government will seek forfeiture in accordance with Title 18, United States Code, Sections 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), which require any person convicted of such offense to forfeit any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly as a result of such offense.

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

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third 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;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendants up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Section 981(a)(1)(C); Title 21, United States Code, Section 853(p); Title 28, United States Code, Section 2461(c))

A TRUE BILL

[redacted]

FOREPERSON

[redacted]

BREON PEACE
UNITED STATES ATTORNEY
EASTERN DISTRICT OF NEW YORK

F.#: 2017R00077
FORM DBD-34
JUN. 85

No.

UNITED STATES DISTRICT COURT

EASTERN *District of* NEW YORK

CRIMINAL DIVISION

THE UNITED STATES OF AMERICA

vs.

NI GAOBIN (倪高彬), WENG MING (翁明), CHENG FENG (程锋), PENG YAOWEN (彭耀文), SUN XIAOHUI (孙小辉), XIONG WANG (熊旺) and ZHAO GUANGZONG (赵光宗),

Defendants.

INDICTMENT

(T. 18, U.S.C. §§ 371, 981(a)(1)(C), 982(a)(2), 982(b)(1), 1030(i)(1), 1030(i)(2), 1349 and 3551 et seq.; T. 21, U.S.C., § 853(p); T. 28, U.S.C., § 2461(c))

A true bill

[redacted]

Foreperson

Filed in open court this _____ *day, of* _____ *A.D. 20* _____

_____
Clerk

Bail, $ _____

Douglas M. Pravda, Saritha Komatireddy, and Jessica K. Weigel, Assistant U.S. Attorneys (718) 254-7000