

**COPY**

FILED

18 OCT 25 PM 3:09

CLERK, U.S. DISTRICT COURT  
SOUTHERN DISTRICT OF CALIFORNIA

BY: *jen* DEPUTY

**SEALED**

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF CALIFORNIA

June 2017 Grand Jury

UNITED STATES OF AMERICA,  
Plaintiff,

v.

ZHANG ZHANG-GUI (1),  
aka "leanov,"  
aka "leaon,"  
ZHA RONG (2),  
CHAI MENG (3),  
aka "Cobain,"  
LIU CHUNLIANG (4),  
aka "sxpdlcl,"  
aka "Fangshou,"  
GAO HONG KUN (5),  
aka "mer4en7y,"  
ZHUANG XIAOWEI (6),  
aka "jpxxav,"  
MA ZHIQI (7),  
aka "Le Ma,"  
LI XIAO (8),  
aka "zhuan86,"  
GU GEN (9),  
aka "Sam Gu,"  
TIAN XI (10),

Defendants.

Case No. 13CR3132-H

I N D I C T M E N T  
**(Superseding)**

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

The grand jury charges:

//

JNP:nlv:(1) San Diego:10/25/18

6

*cc: Pretrial, AUSA Alexandra Foster*

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

1 At various times relevant to this indictment:

2 INTRODUCTION

3 1. The Jiangsu Province Ministry of State Security ("JSSD") was  
4 a provincial foreign intelligence arm of the People's Republic of China's  
5 Ministry of State Security ("MSS"), headquartered in Nanjing, China. The  
6 MSS, and by extension the JSSD, was primarily responsible for domestic  
7 counter-intelligence, non-military foreign intelligence, and aspects of  
8 political and domestic security. From January 2010 to May 2015, JSSD  
9 employees, along with individuals working at the direction of the JSSD,  
10 conspired to steal sensitive commercial technological, aviation, and  
11 aerospace data by hacking into computers in the United States and abroad.

12 2. Supervising and managing officers at JSSD, including  
13 defendants ZHA RONG, CHAI MENG, aka "Cobain," and others, directed  
14 hackers, including ZHANG ZHANG-GUI, aka "leanov," aka "leao," LIU  
15 CHUNLIANG, aka "sxpdlcl," "Fangshou," GAO HONG KUN, aka "mer4en7y,"  
16 ZHUANG XIAOWEI, aka "jpxxav," and MA ZHIQI, aka "Le Ma," as well as  
17 victim company insiders, including GU GEN, aka "Sam Gu," and TIAN XI,  
18 to hack into or facilitate intrusions into computers of companies based  
19 in the United States and abroad for the purpose of gaining and  
20 maintaining unauthorized access to those computers, stealing  
21 information, and using the computers to facilitate additional computer  
22 intrusions.

23 3. Members of the conspiracy targeted, among other things,  
24 companies in the aerospace and other high-technology industries, and  
25 attempted to steal intellectual property and confidential business  
26 information, including information that was commercial in nature.

27 //

28 //

- 1           4.   Members of the conspiracy included, but were not limited to:
- 2           a.   ZHA RONG (查荣 STC<sup>1</sup> 2686/2837), a Division Director in
- 3           the JSSD who supervised and directed human intelligence
- 4           and other activities directed towards the theft of
- 5           intellectual property and confidential business
- 6           information conducted by one or more members of the
- 7           conspiracy. Among other things, ZHA RONG oversaw the
- 8           intrusion into Company I and received updates from one
- 9           or more members of the conspiracy on the day of the
- 10          intrusion.
- 11          b.   CHAI MENG, aka "Cobain," (柴萌 STC 2693/5492), a JSSD
- 12          Section Chief who supervised and directed human
- 13          intelligence and other activities directed towards the
- 14          theft of intellectual property and confidential business
- 15          information conducted by one or more members of the
- 16          conspiracy. Among other things, CHAI MENG served as a
- 17          point of contact to coordinate the activities of hacker
- 18          LIU CHUNLIANG, as well as the activities of victim
- 19          company insiders, during the intrusion into Company I.
- 20          c.   ZHANG ZHANG-GUI, aka "leanov," aka "leao," (张长贵 STC
- 21          1728/7022/6311), a computer hacker who operated at the
- 22          direction of the JSSD. Among other things, ZHANG ZHANG-
- 23          GUI tested spear phishing messages and established and
- 24          maintained infrastructure used in multiple intrusions.
- 25          In addition, as described in detail herein, *infra*, ZHANG

27 \_\_\_\_\_

28 <sup>1</sup> STC is the Standard Telegraphic Code for Chinese, Japanese,  
and Korean characters.

1 coordinated hacking activities and shared infrastructure  
2 with fellow hacker LIU.

3 d. LIU CHUNLIANG, aka "sxpdlcl," "Fangshou," (刘春亮 STC  
4 0491/2504/0081), a computer hacker who operated at the  
5 direction of the JSSD, and coordinated the activities of  
6 other computer hackers and malware developers, including  
7 GAO HONG KUN, aka "mer4en7y," ZHUANG XIAOWEI, aka  
8 "jpxxav," MA ZHIQI, aka "Le Ma," and an identified  
9 unindicted co-conspirator ("UCC-1"). Among other  
10 things, LIU established, maintained and paid for  
11 infrastructure used in multiple intrusions, deployed  
12 malware, and engaged in domain hijacking in connection  
13 with the intrusion of Company H.

14 e. GAO HONG KUN, aka "mer4en7y," (高洪坤 STC 7559/3163/0981),  
15 a computer hacker who operated at the direction of LIU  
16 and was an associate of ZHANG. Among other things, GAO  
17 was involved in the computer intrusions into Capstone  
18 Turbine and Company F.

19 f. ZHUANG XIAOWEI, aka "jpxxav," (庄泉伟 STC 8369/2743/0251),  
20 a computer hacker and malware developer, who operated at  
21 the direction of LIU. Among other things, ZHUANG managed  
22 malware on Company G's systems and stole Company G's data  
23 from no earlier than September 26, 2014, through May 7,  
24 2015.

25 g. MA ZHIQI, aka "Le Ma," (马志琪 STC 7456/1807/3825), a  
26 computer hacker who operated at the direction of LIU and  
27 was a personal acquaintance of LIU and UCC-1. Among  
28 other things, on February 19, 2013, one or more members

1 of the conspiracy hacked into a Company F server  
2 affiliated with LIU, using credentials LIU had provided  
3 to MA on December 14, 2012.

4 h. GU GEN, aka "Sam Gu," (顾根 STC 7357/2704), a Chinese  
5 employee of Company I, a French aerospace manufacturer  
6 with an office in Suzhou, Jiangsu province, China. GU was  
7 Company I's Information Technology ("IT") Infrastructure  
8 and Security Manager in Suzhou. Among other things,  
9 while under the direction of an identified JSSD  
10 intelligence officer ("JSSD Intelligence Officer A"), GU  
11 provided information to JSSD concerning Company I's  
12 internal investigation into the computer intrusions  
13 carried out by members of the conspiracy.

14 i. TIAN XI (田曦 STC 3944/2569), a Chinese employee at  
15 Company I, who worked in its Suzhou office as a Product  
16 Manager. Among other things, TIAN unlawfully installed  
17 Sakula malware on a Company I computer at the behest of  
18 JSSD Intelligence Officer A.

19 5. Members of the conspiracy hacked into protected computers-  
20 that is, computers used in and affecting interstate and foreign commerce  
21 and communications- operated by the following companies, among others,  
22 to steal information, including intellectual property and confidential  
23 business data, and to use these companies' computers to facilitate  
24 further computer intrusions into other companies:

- 25 a. Company A, a Massachusetts-based aerospace company,  
26 b. Company B, an aerospace company based in the United  
27 Kingdom, with offices in Pennsylvania,  
28

- 1 c. Company C, an aerospace company based in the United
- 2 Kingdom, with offices in New York,
- 3 d. Company D, a multinational conglomerate that produces
- 4 commercial and consumer products and aerospace systems,
- 5 e. Company E, a French aerospace company,
- 6 f. Company F, an Arizona-based aerospace company,
- 7 g. Company G, an Oregon-based aerospace supplier,
- 8 h. Company H, a San Diego-based technology company,
- 9 i. Company I, a French aerospace manufacturer with an office
- 10 in Suzhou, Jiangsu province, China,
- 11 j. Company J, a critical infrastructure company operating
- 12 in San Diego and elsewhere,
- 13 k. Company K, a Wisconsin-based aerospace company,
- 14 l. Company L, an Australian domain registrar, and
- 15 m. Capstone Turbines, a Los Angeles-based gas turbine
- 16 manufacturer.

17 6. Members of the conspiracy targeted, among other things, data  
18 and information related to a turbofan engine used in commercial  
19 jetliners. At the time of the intrusions, a Chinese state-owned aerospace  
20 company was working to develop a comparable engine for use in commercial  
21 aircraft manufactured in China and elsewhere. The turbofan engine  
22 targeted by members of the conspiracy was being developed through a  
23 partnership between Company I and an aerospace company based in the U.S.  
24 As described herein, members of the conspiracy hacked Company I and  
25 other companies that manufactured parts for the turbofan engine,  
26 including Companies A, F, and G, to steal sensitive data from these  
27 companies that could be used by Chinese entities to build the same or

28



1 similar engine without incurring substantial research and development  
2 expenses.

3 Count 1

4 7. Paragraphs 1 to 6 are re-alleged and incorporated as if set  
5 forth in full herein.

6 8. From a date unknown, but no later than January 8, 2010, up to  
7 and including May 7, 2015, within the Southern District of California,  
8 and elsewhere, defendants ZHANG ZHANG-GUI, aka "leanov," aka "leacon,"  
9 ZHA RONG, CHAI MENG, aka "Cobain," LIU CHUNLIANG, aka "sxpdlcl,"  
10 "Fangshou," GAO HONG KUN, aka "mer4en7y," ZHUANG XIAOWEI, aka "jpxxav,"  
11 MA ZHIQI, aka "Le Ma," GU GEN, aka "Sam Gu," and TIAN XI did knowingly  
12 and intentionally conspire with each other and other persons known and  
13 unknown to the grand jury to commit an offense against the United States,  
14 that is, to:

- 15 a. cause the transmission of a program, information, code,  
16 and command, and, as a result of such conduct,  
17 intentionally cause damage without authorization to a  
18 protected computer, including loss to at least one person  
19 during a one-year period aggregating at least \$5,000 in  
20 value, in violation of Title 18, United States Code,  
21 Sections 371, 1030(a)(5)(A) and 1030(c)(4)(B)(i); and  
22 b. intentionally access computers without authorization, and  
23 thereby obtain information from at least one protected  
24 computer, such conduct having involved an interstate and  
25 foreign communication, and the offense was committed for  
26 purposes of commercial advantage and private financial  
27 gain and information valued at greater than \$5,000, in  
28

1 violation of 18, United States Code, Sections 371,  
2 1030(a)(2)(C) and 1030(c)(2)(B)(i) and (iii).

3 MANNER AND MEANS

4 9. Members of the conspiracy used the following manner and means,  
5 among others, to accomplish the objects of the conspiracy:

6 a. Certain defendants used email accounts hosted by webmail  
7 providers worldwide, including in the United States and  
8 China. The accounts often used false subscriber  
9 information. Defendants communicated using these email  
10 accounts and often encrypted their communications.

11 b. Certain defendants, directly and through intermediaries,  
12 attempted to hide the nature and origin of their Internet  
13 traffic and reduce the likelihood of detection by leasing  
14 servers or server space worldwide, including in the  
15 United States. Members of the conspiracy forwarded  
16 Internet traffic through multiple such servers using  
17 software to hide the true source and destination of the  
18 traffic.

19 c. Members of the conspiracy used a variety of computer  
20 intrusion tactics, alone or in combination, including but  
21 not limited to:

22 i. Spear phishing, the use of fictitious emails  
23 embedded with malicious code (malware) that  
24 facilitated access to the email recipient's  
25 computer and connected network,

26 ii. Malware, including but not limited to certain  
27 malware, such as Sakula and IsSpace, that was  
28



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27 //  
28 //

uniquely used by members of the conspiracy during the period of the conspiracy,

iii. Doppelganger Domain Names, the creation and use of domain names that closely resemble legitimate domain names to trick unwitting recipients of spear phishing emails,

iv. Dynamic Domain Name Service (DNS) Accounts, a service of DNS providers that allows users, including members of the conspiracy, to register one or more domain names under a single account and frequently change the Internet Protocol (IP) address assigned to a registered domain name.

v. Domain Hijacking, the compromise of domain registrars in which one or more members of the conspiracy redirected a victim company's domain name at a domain registrar to a malicious IP address in order to facilitate computer intrusions,

vi. Watering Hole Attacks, the installation of malware on legitimate web pages of victim companies to facilitate intrusions of computers that visited those pages, and

vii. Co-Opting Victim Company Employees, the use of insiders at victim companies to facilitate computer intrusions or monitor investigations of computer intrusion activity.



1 h. Each of the intrusions of the victim companies described  
2 herein, *infra*, at Paragraph 10, involved malware that was  
3 configured to beacon or otherwise linked to one or more  
4 of these DNS ACCOUNTS between January 2010 and May 2015.

5 Intrusion Into Capstone Turbine Computers

6 i. On January 8, 2010, members of the conspiracy infiltrated  
7 the Capstone Turbine computer network, created an email  
8 account in the Capstone Turbine email server, and tested  
9 a potential spear phishing email by sending an email from  
10 the newly-created Capstone Turbine email account to  
11 ZHANG's personal email account.

12 j. On May 24, 2012, a member of the conspiracy installed  
13 malware on Capstone Turbine's web server to facilitate a  
14 watering hole attack.

15 k. On or before May 24, 2012, a member of the conspiracy  
16 installed Winnti malware in Capstone Turbine's computer  
17 systems, and the malware, as programmed, sent "beacons"  
18 to domain names hosted by DNS ACCOUNT-1, as well as to a  
19 blog controlled by "mer4en7y," which is an alias used by  
20 GAO. Malware is designed to "beacon" in order to, among  
21 other things, notify members of the conspiracy that the  
22 malware has been successfully installed.

23 l. On or about May 30, 2012, a server associated with ZHANG,  
24 which was located in Nanjing, China, was used to gain  
25 unauthorized access to Capstone Turbine's web server.

26 m. On May 31, 2012, a member of the conspiracy used the IP  
27 address of a server associated with ZHANG to connect to  
28 the Capstone Turbine web server using a Capstone Turbine

1 administrative account with system administrator  
2 privileges (which meant the account user had access to  
3 most areas of the Capstone Turbine network).

4 n. On June 1, 2012, a member of the conspiracy used the same  
5 administrative account to upload malware to Capstone  
6 Turbine's web server for use in a watering hole attack.

7 o. On August 23, 2012, ZHANG tested a potential spear  
8 phishing email that used the doppelganger domain name  
9 capstonetrubine.com (emphasis added). At that time, the  
10 doppelganger domain name capstonetrubine.com was  
11 registered to DNS ACCOUNT-2.

12 p. On or before December 29, 2012, members of the conspiracy  
13 caused Sakula malware on Capstone Turbine's server to  
14 send a beacon to an account under the control of one or  
15 more members of the conspiracy.

16 Intrusion Into Company F's Computers

17 q. On May 30, 2012, a member of the conspiracy caused malware  
18 to be installed on Company F's computer network through  
19 a spear phishing attack, which contained a link to a  
20 domain on DNS ACCOUNT-2. Company F manufactured parts  
21 for the turbofan engine developed by Company I and an  
22 aerospace company based in the U.S.

23 r. On June 8, 2012, a member of the conspiracy first accessed  
24 a specific Company F server (the "Compromised Company F  
25 Server").

26 s. On December 14, 2012, LIU gave MA directions on how to  
27 hack into the Compromised Company F Server. LIU provided  
28 MA with LIU's credentials to access the server and

1 provided guidance as to how MA could package and steal  
2 data from the server to minimize detection.

3 t. On February 19, 2013, a member of the conspiracy accessed  
4 the Compromised Company F Server, created a compressed  
5 file of Company F's confidential data, and saved it on  
6 Company F's server, using the IP address, username,  
7 password and methodology, which LIU had provided to MA  
8 on December 14, 2012.

9 u. On March 18, 2013, LIU gave GAO the IP address assigned  
10 to a domain name under the control of one or more members  
11 of the conspiracy, so GAO could access the malware  
12 installed within Company F's computer network.

13 v. Between June 8, 2012 and May 9, 2013, LIU, GAO, MA, and  
14 other members of the conspiracy accessed Company F's  
15 server for the purpose of stealing data related to  
16 Company F's products.

17 Intrusion Into Company H's Computers

18 w. No later than August 7, 2012, a member of the conspiracy  
19 caused malware to be installed on Company H's computer  
20 network.

21 x. On or before August 23, 2012, a member of the conspiracy  
22 caused PlugX malware named "capstone.exe" to be installed  
23 in Company H's computer systems to send beacons to four  
24 domain names registered to DNS ACCOUNT-1, including  
25 doppelganger domain name "capstoneturbine.cechire.com."

26 y. On August 28, 2013, LIU sent MA a link to a news article  
27 that explained how the Syrian Electronic Army (SEA) had  
28

1 hacked into the computer systems of Company L, a domain  
2 registrar, in order to facilitate intrusions.

3 z. On December 3, 2013, members of the conspiracy used the  
4 same method as the SEA to hack into the computer systems  
5 of Company L and hijack domain names of Company H, which  
6 were hosted by Company L.

7 aa. On December 3, 2013, a member of the conspiracy installed  
8 Sakula malware on Company H's computer network and caused  
9 the malware to send a beacon to a doppelganger domain  
10 name under the control of one or more members of the  
11 conspiracy. Notably, the doppelganger domain name was  
12 designed to resemble the real domain of Company A, which  
13 had previously been hacked by members of the conspiracy.

14 bb. Between December 3, 2013, and January 15, 2014, members  
15 of the conspiracy accessed approximately 40 computer  
16 systems operated by Company H and installed a variety of  
17 malware, including Sakula, Winnti, and PlugX, to steal  
18 Company H's data.

19 Intrusion Into Company I's Computers

20 cc. In mid-November 2013, JSSD Intelligence Officer A met  
21 TIAN, an employee of Company I, at a restaurant in Suzhou,  
22 Jiangsu province, China. The turbofan engine targeted  
23 by members of the conspiracy was being developed through  
24 a partnership between Company I and an aerospace company  
25 based in the U.S.

26 dd. On November 27, 2013, JSSD Intelligence Officer A  
27 communicated to TIAN, in substance and in part, "I'll  
28 bring the horse [i.e., Trojan horse malware] to you

1                    tonight. Can you take the Frenchmen out to dinner  
2                    tonight? I'll pretend I bump into you at the restaurant  
3                    to say hello. This way we don't need to meet in Shanghai."  
4 ee. On November 27, 2013, TIAN met JSSD Intelligence Officer  
5                    A at a restaurant.  
6 ff. In December 2013, JSSD Intelligence Officer A contacted  
7                    TIAN three times and asked, in substance and in part, if  
8                    TIAN had "plant[ed] the horse."  
9 gg. On January 17, 2014, JSSD Intelligence Officer A met GU,  
10                    the IT Infrastructure and Security Manager for Company  
11                    I, at the same restaurant where he had previously met  
12                    TIAN.  
13 hh. JSSD Intelligence Officer A and CHAI coordinated with  
14                    each other and provided same-day updates to their  
15                    colleagues and superiors, including ZHA, on the targeting  
16                    of and intrusion into Company I.  
17 ii. On January 17, 2014, JSSD Intelligence Officer A informed  
18                    CHAI, in substance and in part, "I just met with Xiao GU.  
19                    GU said that [Company I] was warning people about a fake  
20                    email from company top management. Did you guys write the  
21                    email?" CHAI responded, in substance and in part, "We  
22                    sent a fake email pretending to be from network  
23                    management."  
24 jj. On January 17, 2014, JSSD Intelligence Officer A informed  
25                    CHAI that he told GU that CHAI's group had sent the email.  
26 kk. On January 25, 2014, a Company I laptop computer was  
27                    infected with Sakula malware through a USB drive  
28                    installed by TIAN, which beacons to a doppelganger



1 domain name under the control of one or more members of  
2 the conspiracy during that period. Notably, this was the  
3 same doppelganger domain designed to resemble the real  
4 domain of Company A, which members of the conspiracy had  
5 used when hacking into Company H.

6 11. On January 25, 2014, TIAN texted JSSD Intelligence  
7 Officer A, "The horse was planted this morning." Shortly  
8 thereafter, JSSD Intelligence Officer A texted CHAI with  
9 a message that read, in part: "I briefed ZHA about the  
10 incident in Suzhou."

11 mm. On February 19, 2014, a Company I computer beacons to  
12 domain ns24.dnsdojo.com, which was then managed by DNS  
13 ACCOUNT-3. Shortly thereafter, U.S. law enforcement  
14 authorities notified French officials of the beacon  
15 activity.

16 nn. On February 26, 2014, JSSD Intelligence Officer A texted  
17 CHAI, "The French are asking Little GU [Company I's IT  
18 manager] to inspect the record: ns24.dnsdojo.com. Does  
19 it concern you guys?" CHAI responded, "I'll ask."

20 oo. Several hours after that text exchange, a member of the  
21 conspiracy logged into DNS ACCOUNT-3, an account  
22 controlled by LIU, and deleted the domain name  
23 ns24.dnsdojo.com.

#### 24 Intrusion Into Company G's Computers

25 pp. On September 25, 2014, ZHUANG created a Google AppEngine  
26 account named "apple-qts."

27 qq. On September 26, 2014, members of the conspiracy caused  
28 malware to be installed on at least one Company G computer

1 through a watering hole attack hosted on a Company I  
2 domain. Company G manufactured parts for the turbofan  
3 engine developed by Company I and an aerospace company  
4 based in the U.S.

5 rr. On March 28, 2015, members of the conspiracy caused a  
6 computer belonging to Company G to beacon to a domain  
7 registered to DNS ACCOUNT-4.

8 ss. ZHUANG used his apple-qts Google AppEngine account to  
9 manage malware, including IsSpace, on Company G's systems  
10 and steal commercial data from Company G from no earlier  
11 than September 26, 2014, through May 7, 2015.

12 All in violation of Title 18, United States Code, Sections 371,  
13 1030(a)(5)(A), 1030(c)(4)(B)(i), 1030(a)(2)(C) and 1030(c)(2)(B)(i)  
14 and (iii).

15 Count 2

16 11. Paragraphs 1 to 10 are re-alleged and incorporated as if set  
17 forth in full herein.

18 12. From a date unknown, but no later than September 3, 2012, up  
19 to and including February 11, 2014, within the Southern District of  
20 California, and elsewhere, defendants ZHANG ZHANG-GUI, aka "leanov,"  
21 aka "leaon," and LI XIAO, aka "zhuan86," did knowingly and intentionally  
22 conspire with each other and other persons known and unknown to the  
23 grand jury to commit an offense against the United States, that is, to:

24 a. cause the transmission of a program, information, code,  
25 and command, and, as a result of such conduct,  
26 intentionally cause damage without authorization to a  
27 protected computer, including loss to at least one person  
28 during a one-year period aggregating at least \$5,000 in

1 value, in violation of Title 18, United States Code,  
2 Sections 371, 1030(a)(5)(A) and 1030(c)(4)(B)(i); and  
3 b. intentionally access one and more computers without  
4 authorization, and thereby obtain information from at  
5 least one protected computer, such conduct having  
6 involved an interstate and foreign communication, and the  
7 offense was committed for purposes of commercial  
8 advantage and private financial gain and information  
9 valued greater than \$5,000, in violation of 18, United  
10 States Code, Sections 371, 1030(a)(2)(C) and  
11 1030(c)(2)(B)(i) and (iii).

12 13. LI XIAO, aka "zhuan86," (李潇 STC 2621/3469), is a computer  
13 hacker and a personal friend of ZHANG ZHANG-GUI, aka "leanov,"  
14 aka "leaon". ZHANG supplied LI with variants of the malware that had  
15 been developed and deployed by members of the separate JSSD-related  
16 conspiracy charged in Count 1, as described herein, *supra*, at Paragraphs  
17 7 through 10. LI subsequently used malware that had been supplied by  
18 ZHANG, as well as other malware, in his attempts to hack into Company  
19 H's computers, which ZHANG and others had also targeted in the separate  
20 conspiracy charged in Count 1.

21 OVERT ACTS

22 Intrusion Into Company H's Computers

23 14. In furtherance of the conspiracy and to effect the objects  
24 thereof, the following overt acts, among others, were committed within  
25 the Southern District of California and elsewhere, on or about the dates  
26 below:

27 //

28 //

- 1 a. On September 3, 2012, ZHANG emailed LI a set of malicious  
2 files, that was a subset of the malware installed on  
3 Capstone Turbine's web server on June 1, 2012, as  
4 described herein, *supra*, at Paragraph 10(n).
- 5 b. On or about October 27, 2012, LI created a Google  
6 AppEngine application to facilitate computer intrusions.
- 7 c. On September 11, 2013, a web shell or script was installed  
8 on a web server operated by Company H, which allowed a  
9 user to gain remote administrative control of Company H's  
10 server.
- 11 d. On or before September 29, 2013, a second web shell was  
12 installed on the same web server to facilitate computer  
13 intrusion activities on Company H's server.
- 14 e. On or about September 29, 2013, LI used the Google  
15 AppEngine application to access the second shell on  
16 Company H's server. LI did so in order to leverage the  
17 hack of Company H's server into intrusions of other  
18 victims.
- 19 f. On or about October 10, 2013, LI attempted to use one of  
20 the shells to gain access to a third-party website.
- 21 g. On or about February 11, 2014, LI installed malicious  
22 code on a Company H server to exploit an Internet Explorer  
23 vulnerability, which had previously been used by ZHANG  
24 and other members of the conspiracy described herein,  
25 *supra*, at Paragraphs 7 through 10.

26 All in violation of Title 18, United States Code, Sections 371,  
27 1030(a)(5)(A), 1030(c)(4)(B)(i), 1030(a)(2)(C) and 1030(c)(2)(B)(i)  
28 and (iii).

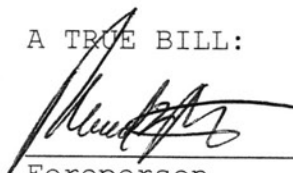


1 the United States of America shall be entitled to forfeit substitute  
2 property pursuant to Title 21, United States Code, Section 853(p), as  
3 incorporated by Title 18, United States Code, Section 982(b)(1).

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

6 DATED: October 25, 2018.

7 A TRUE BILL:

8 

9 Foreperson

10 ADAM L. BRAVERMAN  
11 United States Attorney

12  
13 By:



14 TIMOTHY F. SALEL  
Assistant U.S. Attorney