

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

UNITED STATES OF AMERICA

v.

Criminal No. 14-118

WANG DONG, a/k/a "Jack Wang,"
a/k/a "UglyGorilla,"
SUN KAILIANG, a/k/a "Sun Kai
Liang," a/k/a "Jack Sun,"
WEN XINYU, a/k/a "Wen Xin Yu,"
a/k/a "WinXYHappy," a/k/a
"Win_XY," a/k/a "Lao Wen,"
HUANG ZHENYU, a/k/a "Huang Zhen
Yu," a/k/a "hzy_lhx,"
GU CHUNHUI, a/k/a "Gu Chun
Hui," a/k/a "KandyGoo,"

UNDER SEAL

FILED

MAY - 1 2014

CLERK U.S. DISTRICT COURT
WEST. DIST. OF PENNSYLVANIA

INDICTMENT MEMORANDUM

AND NOW comes the United States of America, by its attorneys, David J. Hickton, United States Attorney for the Western District of Pennsylvania, and James T. Kitchen, Assistant United States Attorney for said District, and submits this Indictment Memorandum to the Court:

I. THE INDICTMENT

A Federal Grand Jury returned a 31-count Indictment against the above-named defendants for alleged violations of federal law:

<u>COUNT</u>	<u>OFFENSE/DATE</u>	<u>TITLE/SECTION</u>	<u>DEFENDANTS CHARGED</u>
1	Conspiracy to Commit Computer Fraud, from in or about 2010 to in or about April 2014	18 U.S.C. § 1030(b)	All defendants

<u>COUNT</u>	<u>OFFENSE/DATE</u>	<u>TITLE/SECTION</u>	<u>DEFENDANTS CHARGED</u>
2-9	Intentionally Accessing and Obtaining Information from a Protected Computer, on various dates from on or about February 26, 2010 to on or about April 13, 2012	18 U.S.C. § 1030(a)(2)(C) & (c)(2)(B)(i)-(iii)	All defendants
10-23	Intentional Damage to a Protected Computer, on various dates from on or about February 8, 2010 to on or about April 13, 2012	18 U.S.C. § 1030(a)(5)(A) & (c)(4)(B)	All defendants
24-29	Aggravated Identity Theft, from on or about December 30, 2010 to on or about April 13, 2012	18 U.S.C. § 1028A(a)(1), (b), & (c)(4)	All defendants
30	Economic Espionage, on or about May 6, 2010	18 U.S.C. § 1831(a)(2) & (4)	All defendants
31	Theft of Trade Secrets, on or about May 6, 2010	18 U.S.C. § 1832(a)(2) & (4)	All defendants

II. ELEMENTS OF THE OFFENSES

A. As to Count 1: In order for the crime of **Conspiracy to Commit Computer Fraud**, in violation of 18 U.S.C. § 1030(b), to be established, the government must prove all of the following essential elements beyond a reasonable doubt:

1. That two or more persons agreed to commit an offense set forth under subsection (a) of Title 18, United States Code, Section 1030;

2. That the defendants were a party to or member of that agreement;

3. That the defendants joined the agreement or conspiracy knowing of its objective to commit an offense in violation of subsection (a) of 18 U.S.C. § 1030, and intending to join together with at least one other alleged conspirator to achieve those objectives; that is, that the defendants and at least one other alleged conspirator shared a unity of purpose and the intent to achieve common goals or objectives, to commit an offense in violation of subsection (a) of 18 U.S.C. § 1030.

B. As to Counts 2-9: In order for the crime of **Illegal Access and Obtaining Information from a Protected Computer**, in violation of 18 U.S.C. § 1030(a)(2) & (c)(2)(B)(i)-(iii), to be established, the government must prove all of the following essential elements beyond a reasonable doubt:

1. The defendants intentionally accessed a computer without authorization or in excess of authorization;

2. That the defendants obtained thereby the information in the relevant count;

3. From a "protected computer;" and

4. That the offense:

a. Was committed for purposes of commercial advantage or private financial gain;

b. Was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

c. Involved the obtaining of information exceeding \$5,000 in value.

C. As to Counts 10-23: In order for the crime of **Intentional Damage to a Protected Computer**, in violation of 18 U.S.C. § 1030(a)(5)(A) & (c)(4)(B), to be established, the government must prove all of the following essential elements beyond a reasonable doubt:

1. That the defendants knowingly caused transmission of a program, information, or command;

2. That, as a result of such transmission, the defendants intentionally caused damage to a protected computer;

3. The damage caused by the defendants was without authorization; and

4. That the offense resulted in a loss of \$5,000 during one year, or the damage affected ten or more protected computers during one year.

D. As to Counts 24-29: In order for the crime of **Aggravated Identity Theft**, in violation of 18 U.S.C. § 1028A(a)(1), (b), (c)(4), to be established, the government must prove all of the following essential elements beyond a reasonable doubt:

1. That the defendants violated the Computer Fraud and Abuse Act, as charged in Count One;

2. That the defendants, during and in relation to that conspiracy, knowingly transferred, possessed or used, a "means of identification;"

3. Without lawful authority; and

4. Which means of identification belonged to another person.

18 U.S.C. § 1028A(a)(1).

E. As to Count 30: In order for the crime of **Economic Espionage**, in violation of 18 U.S.C. § 1831(a)(2) & (4), to be established, the government must prove all of the following essential elements beyond a reasonable doubt:

1. That the defendants, intending or knowing that an offense will benefit any foreign government, foreign instrumentality, or foreign agent;

2) Knowingly stole or without authorization appropriated information (including through copying and downloading); and

3. That the defendants knew or had a firm belief that the information was a trade secret;

4. **(Except in the case of an attempt)** That the information was, in fact, a trade secret.

F. As to Count 31: In order for the crime of **Theft of Trade Secrets**, in violation of 18 U.S.C. § 1832(a)(2) & (4), to be established, the government must prove all of the following essential elements beyond a reasonable doubt:

1. That the defendants, knowing or intending that an offense would economically benefit someone other than the owner thereof;

2. Knowingly stole or without authorization appropriated information (including through copying and downloading);

3. That the defendants knew or had a firm belief that the information was a trade secret;

4. The defendants acted with the knowledge or intent that the offense would injure the trade secret owner.

5. **(Except in cases of attempt)** that the information taken or possessed was a trade secret; and

6. That the trade secret was related to or included in a product that was produced for or placed in interstate or foreign commerce.

G. Pinkerton Liability

For a defendant to be guilty of a substantive crime based on *Pinkerton* liability, the Government must prove:

1. That the defendant was a member of the conspiracy charged in the indictment;

2. That while the defendant was still a member of the conspiracy, one or more of the other members of the conspiracy committed the substantive offense charged in the relevant count, by committing each of the elements of that offense;

3. That the other members of the conspiracy committed this offense within the scope of the unlawful agreement and to help further or achieve the objective(s) of the conspiracy; and

4. That these offenses were reasonably foreseeable to or reasonably anticipated by the defendant as necessary or natural consequences of the unlawful agreement.

The government does not have to prove that the defendants specifically agreed or knew that this offense would be committed. However, the government must prove that the offense was reasonably foreseeable to the defendants, as a member of the conspiracy, and within the scope of the agreement as the defendants understood it.

Third Circuit Model Jury Instruction 7.03.

H. Accomplice Liability: Aiding and Abetting (18 U.S.C. § 2)

In order to find a defendant guilty of an offense he or she aided or abetted, the government must prove:

1. That the alleged principal committed the offenses charged by committing each of the elements of the offenses charged.

2. That the defendant knew that the offenses charged was going to be committed or was committed by the principal;

3. That the defendant knowingly did some act for the purpose of aiding, assisting, soliciting, facilitating, or encouraging the alleged principal to commit the specific

offenses charged and with the intent that the alleged principal commit those specific offenses; and

4. That the defendant's acts did, in some way, aid, assist, facilitate, or encourage the alleged principal to commit the offense. The defendant's acts need not themselves be against the law.

Third Circuit Model Jury Instruction 7.02.

III. PENALTIES

A. As to Count 1: Conspiracy to Commit Computer Fraud (18 U.S.C. § 1030(b)); Multi-Object Conspiracy to violate 18 U.S.C. § 1030(a)(2)(C) and (c)(2)(B)(i)-(iii) and 18 U.S.C. § 1030(a)(5)(A) & (c)(4)(B):

In the case of a conviction on a Conspiracy to violate 18 U.S.C. § 1030(a)(2)(C) and (c)(2)(B)(i)-(iii):

1. Individuals - The maximum penalties for individuals are:

(a) a term of imprisonment of not more than 5 years;

(b) a fine of up to \$250,000 or twice the pecuniary gain to any person or twice the pecuniary loss to any person;

(c) A term of supervised release of not more than three years.

(d) Any or all of the above.

In the case of a conviction on a Conspiracy to violate 18 U.S.C. § 1030(a) (5) (A) and (c) (4) (B) :

1. Individuals - The maximum penalties for individuals are:

(a) a term of imprisonment of not more than 10 years;

(b) a fine of up to \$250,000 or twice the pecuniary gain to any person or twice the pecuniary loss to any person;

(c) A term of supervised release of not more than three years.

(d) Any or all of the above.

B. As to Counts 2-9: Illegal Access and Obtaining Information from a Protected Computer (18 U.S.C. § 1030(a) (2) (c) & (c) (2) (B) (i)-(iii)) :

1. A term of imprisonment of not more than 5 years;

2. A fine of up to \$250,000 or twice the pecuniary gain to any person or twice the pecuniary loss to any person;

3. A term of supervised release of not more than three years.

C. As to Counts 10-23: Intentional Damage to a Protected Computer (18 U.S.C. § 1030(a) (5) (A) & (c) (4) (B)) :

1. A term of imprisonment of not more than 10 years;

2. A fine of up to \$250,000 or twice the pecuniary gain to any person or twice the pecuniary loss to any person;

3. A term of supervised release of not more than three years.

D. As to Counts 24-29: Aggravated Identity Theft (18 U.S.C. § 1028A(a) (1), (b), (c) (4)):

1. A mandatory term of imprisonment of two years to run consecutively with any other term of imprisonment imposed, except as stated in 18 U.S.C. § 1028A(b)(4) (18 U.S.C. § 1028A(a)(1), (b));

2. A fine of up to \$250,000 or twice the pecuniary gain or loss to any person;

3. A term of supervised release of not more than one (1) year;

4. Any or all of the above.

E. As to Count 30: Economic Espionage (18 U.S.C. § 1831(a) (2)):

1. A term of imprisonment of not more than 15 years;

2. A fine of up to \$5,000,000;

3. A term of supervised release of not more than three years.

F. As to Count 31: Theft of Trade Secrets (18 U.S.C. § 1832(a) (2) & (4)):

1. A term of imprisonment of not more than 10 years;

2. A fine of up to \$250,000 or twice the pecuniary gain to any person or twice the pecuniary loss to any person;

3. A term of supervised release of not more than three years.

IV. MANDATORY SPECIAL ASSESSMENT

A mandatory special assessment of \$100.00 must be imposed at each count upon which the defendant is convicted, pursuant to 18 U.S.C. § 3013.

V. RESTITUTION

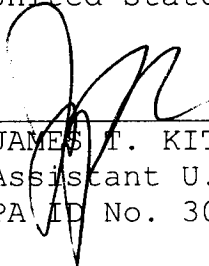
Restitution may be required in this case as to all Counts, together with any authorized penalty, as part of the defendants' sentence pursuant to 18 U.S.C. §§ 3663, 3663A, and 3664.

VI. FORFEITURE

Not applicable in this case.

Respectfully submitted,

DAVID J. HICKTON
United States Attorney



JAMES T. KITCHEN
Assistant U.S. Attorney
PA ID No. 308565