

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

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

June 2011 Grand Jury

CR 11 00848

UNITED STATES OF AMERICA,
Plaintiff,
v.
CODY ANDREW KRETSINGER,
aka "recursion,"
Defendant.

CR No. 11-00848
I N D I C T M E N T
[18 U.S.C. § 371: Conspiracy; 18
U.S.C. §§ 1030(a)(5)(A),
(c)(4)(B)(i), (c)(4)(A)(i)(I):
Unauthorized Impairment of a
Protected Computer]

The Grand Jury charges:

INTRODUCTORY ALLEGATIONS

1. At all times relevant to this Indictment:
a. Sony Pictures Entertainment, Inc. ("Sony Pictures"), a subsidiary of Sony Corporation of America, was a major motion picture and television production company located within the Central District of California. Sony Pictures maintained computer systems, including database servers and servers for hosting its website (www.sonypictures.com), in Los Angeles County, within the Central District of California.

1 b. "Anonymous" was a collective of computer hackers
2 and other individuals located throughout the world, including the
3 United States, that conducted cyber attacks against individuals
4 and entities that were perceived to be hostile to Anonymous and
5 its members' interests. These attacks included, among other
6 things, the theft and later dissemination of confidential
7 information from victims' computer systems.

8 c. "Lulz Security," or simply "LulzSec," was a group
9 of elite computers hackers affiliated with Anonymous. LulzSec
10 undertook cyber attacks on the computer systems of various
11 business and government entities in the United States and
12 throughout the world. LulzSec announced and published
13 confidential information it had stolen during such attacks on its
14 website, lulzsecurity.com, and via its Twitter account, @LulzSec.

15 d. Defendant CODY ANDREW KRETSINGER, also known as
16 "recursion" ("defendant"), resided in Tempe, Arizona, within the
17 District of Arizona, and was a member of LulzSec who went by the
18 username "recursion."

19 e. The website hidemyass.com was an online service
20 provider that offered proxy services, including via virtual
21 private network ("VPN"), that purportedly allowed its users to
22 use the Internet anonymously. Hidemyass.com maintained proxy
23 servers in numerous countries, including in the United States.

24 2. The following definitions apply to this Indictment:

25 a. "SQL," or "Structured Query Language," is a
26 widely-used database language designed to manage data in a
27 database and includes commands to extract, insert, update, and
28 delete data.

1 b. A "SQL injection attack" is a form of attack on a
2 database-driven website in which the attacker executes
3 unauthorized SQL commands and takes advantage of insecure code on
4 a computer system connected to the Internet. SQL injection
5 attacks are often used to steal information from a database from
6 which the data would normally not be available and to gain access
7 to an organization's computers systems through the computer that
8 is hosting the database.

9 c. A "proxy server" is a computer system or
10 application that acts as an intermediary for requests from
11 clients seeking resources from other servers. A proxy server has
12 a large variety of potential uses, one of which is to attempt to
13 hide one's true Internet Protocol or "IP" address from others,
14 and to thereby remain anonymous.

COUNT ONE

[18 U.S.C. § 371]

3. The Grand Jury re-alleges and incorporates by reference the introductory allegations set forth in paragraphs one and two of this Indictment.

A. THE SCHEME TO DEFRAUD

4. Beginning on a date unknown and continuing through in or about June 2011, in Los Angeles County, within the Central District of California, and elsewhere, defendant, together with others known and unknown to the Grand Jury, knowingly combined, conspired, and agreed to commit the following offense against the United States: To impair and cause damage to a protected computer without authorization, in violation of Title 18, United States Code, Section 1030(a)(5)(A).

B. THE MANNER AND MEANS OF THE CONSPIRACY

5. The object of the conspiracy was carried out, and to be carried out, in substance, as follows:

a. Defendant would register for a proxy service at hidemyass.com to attempt to hide his Internet activities from others.

b. Defendant, together with known and unknown coconspirators, would probe Sony Pictures' computer systems for vulnerabilities that could be exploited through a SQL injection attack.

c. Defendant, together with known and unknown coconspirators, would conduct a SQL injection attack against Sony Pictures' computer systems.

1 d. Defendant, together with known and unknown
2 coconspirators, would obtain confidential information from Sony
3 Pictures' computer systems as a result of the SQL injection
4 attack.

5 e. Defendant would distribute to other members of
6 LulzSec the confidential information he had stolen from Sony
7 Pictures' computer systems.

8 f. Defendant, together with known and unknown
9 coconspirators, would announce the attack against Sony Pictures'
10 computer systems on LulzSec's lulzsecurity.com website and via
11 its @LulzSec Twitter account.

12 g. Defendant, together with known and unknown
13 coconspirators, would post confidential information stolen from
14 Sony Pictures on LulzSec's lulzsecurity.com website.

15 h. To destroy evidence, defendant would wipe, that
16 is, permanently erase, the hard drive of the computer with which
17 defendant had conducted the attack against Sony Pictures'
18 computer systems.

19 C. OVERT ACTS

20 6. In furtherance of the conspiracy, and to accomplish its
21 object, defendant, together with others known and unknown to the
22 Grand Jury, committed and willfully caused others to commit the
23 following overt acts, among others, in the Central District of
24 California and elsewhere:

25 Overt Act No. 1: On or about May 23, 2011, defendant
26 registered for a virtual private network account at hidemyass.com
27 and chose the username "recursion."
28

1 Overt Act No. 2: On or about May 27, 2011, defendant and
2 other known and unknown coconspirators probed Sony Pictures'
3 computer systems for vulnerabilities that could be exploited
4 through a SQL injection attack.

5 Overt Act No. 3: From on or about May 30, 2011, through on
6 or about June 2, 2011, defendant and other known and unknown
7 coconspirators conducted a SQL injection attack against Sony
8 Pictures' computer systems, exploiting vulnerabilities in such
9 systems and making tens of thousands of requests for confidential
10 data.

11 Overt Act No. 4: From on or about May 30, 2011, through on
12 or about June 2, 2011, defendant and other known and unknown
13 coconspirators stole confidential data from Sony Pictures'
14 computer systems via a SQL injection attack.

15 Overt Act No. 5: On and before June 2, 2011, defendant
16 provided confidential information he had stolen from Sony
17 Pictures' computer systems via a SQL injection attack to other
18 members of LulzSec.

19 Overt Act No. 6: On or about June 2, 2011, defendant and
20 other known and unknown coconspirators announced the attack
21 against Sony Pictures on LulzSec's lulzsecurity.com website and
22 via its @LulzSec Twitter account.

23 Overt Act No. 7: On or about June 2, 2011, defendant and
24 other known and unknown coconspirators posted the confidential
25 information stolen from Sony Pictures on LulzSec's
26 lulzsecurity.com website.

27 Overt Act No. 8: On or after June 2, 2011, defendant wiped,
28 that is, permanently erased, the hard drive of the computer with

1 which defendant conducted the SQL injection attack against Sony
2 Pictures' computer systems.

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

COUNT TWO

[18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I)]

7. The Grand Jury re-alleges and incorporates by reference the allegations set forth in paragraphs one, two, and five of this Indictment.

8. From on or about May 27, 2011, through on or about June 2, 2011, in Los Angeles County, within the Central District of California, and elsewhere, defendant knowingly caused the transmission of programs, information, codes, and commands, and as a result of such conduct, intentionally caused damage without authorization by impairing the integrity and availability of data, programs, systems, and information on a computer system that was used in and affecting interstate and foreign commerce and communication, specifically, Sony Pictures' computer systems located in Los Angeles County, California, thereby causing a loss

///

///

///

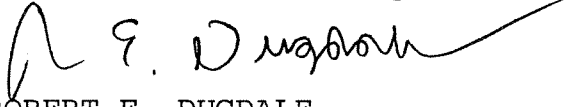
1 to Sony Pictures aggregating at least \$5,000 in value during a
2 one-year period beginning on or about May 27, 2011.

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

A TRUE BILL

15/
Foreperson

ANDRÉ BIROTTE JR.
United States Attorney



ROBERT E. DUGDALE
Assistant United States Attorney
Chief, Criminal Division

WESLEY L. HSU
Assistant United States Attorney
Chief, Cyber & Intellectual Property Crimes Section

ERIC D. VANDEVELDE
Assistant United States Attorney
Deputy Chief, Cyber & Intellectual Property Crimes Section

STEPHANIE S. CHRISTENSEN
Assistant United States Attorney
Cyber & Intellectual Property Crimes Section