FILED

2012 JUN 12 PM 4:04

CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
LOS ANGELES

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

February 2012 Grand Jury

UNITED STATES OF AMERICA,	)	CR No. 12- CR12-0561
Plaintiff,	)	
	)	I N D I C T M E N T
v.	)	
	)	[18 U.S.C. § 371: Conspiracy;
RYAN CLEARY,	)	18 U.S.C. §§ 1030(a)(5)(A),
	)	(c)(4)(B)(i), (c)(4)(A)(i)(I):
Defendant.	)	Unauthorized Impairment of a
	)	Protected Computer]
	)	
	)	
	)	

The Grand Jury charges:

INTRODUCTORY ALLEGATIONS

    1.   The following definitions apply to this Indictment:

        a.   Botnet: A "botnet" is a collection of compromised computers, known as "bots," that autonomously respond to and execute commands issued by the botnet's owner, often for nefarious purposes. Computers become part of a botnet by being infected with malicious software, known as "malware," which may install itself on a user's computer without the user's knowledge, often by taking advantage of web browser vulnerabilities or by

1 tricking the user into running a Trojan horse program. Once the

2 computer is infected and becomes a bot in the botnet, the malware

3 can listen for, respond to, and execute commands issued by the

4 botnet's owner, for example, to make connections to a particular

5 server as part of a distributed denial of service, or "DDoS,"

6 attack.

7   b.   DDoS attack: A "DDoS attack" is a type of

8 malicious computer activity that attempts to render a computer

9 resource unavailable to its intended users by flooding it with

10 large amounts of data or commands. As a result, the victim

11 computer is unable to handle legitimate network traffic, and

12 legitimate users are denied the services of the computer

13 resource. One common method of attack involves saturating the

14 target computer with external communications requests, such that

15 it cannot respond to legitimate traffic or responds so slowly as

16 to be rendered effectively unavailable. For example, a DDoS

17 attack against a website server might flood the server with so

18 many webpage requests that the server can no longer respond to

19 legitimate traffic. Depending on the type and strength of the

20 DDoS attack, the victim computer and its network may become

21 completely disabled and unable to perform their intended

22 functions without significant repair. A DDoS attack is

23 "distributed" in nature if the flood of data and/or commands sent

24 to the target machine originates from a large number of

25 computers, for example, when the owner of a botnet directs all of

26 the bots in the botnet to send requests to the same server at the

27 same time.

28

1   2.   At all times relevant to this Indictment:

2   a.   DreamHost ("DreamHost"), a subsidiary of New Dream

3   Network, LLC, was a data and server hosting company located

4   within the Central District of California that provided shared,

5   dedicated, and virtual private server hosting services to

6   numerous individuals and businesses. DreamHost leased server

7   space and computing resources for use by its clients, as well as

8   provided Internet connectivity, typically in a data center.

9   DreamHost maintained computer systems, including its own and

10 those used to provide hosting services, in Los Angeles,

11 California.

12   b.   "Anonymous" was a collective of computer hackers

13 and other individuals located throughout the world, including the

14 United States, that conducted cyber attacks against individuals

15 and entities that were perceived to be hostile to Anonymous and

16 its members' interests. These attacks included, among other

17 things, the theft and later dissemination of confidential

18 information from victims' computer systems.

19   c.   "Lulz Security," or simply "LulzSec," was a group

20 of computers hackers affiliated with Anonymous. LulzSec

21 conducted cyber attacks against the computer systems of various

22 corporate and government entities in the United States and

23 throughout the world.

24   d.   Defendant RYAN CLEARY ("defendant CLEARY"), a

25 resident and citizen of the United Kingdom, was a member of and

26 affiliated with various hacking groups, including Anonymous and

27 LulzSec.

28

1   i.   Defendant CLEARY used the following online
2 nicknames and usernames, and variants thereof, including, among
3 others, "ryan," "herschel.mcdoogenstein," "anakin,"
4 "evanwarwick," "francis madsen," "george hampsterman," "ni,"
5 "viral," and "x."
6   ii.   Defendant CLEARY developed software for, and
7 maintained and controlled a large botnet, comprised of tens of
8 thousands, and potentially hundreds of thousands, of bots.
9 Defendant CLEARY used his botnet to conduct DDoS attacks against
10 various corporate and government entities, including DreamHost.
11 Defendant CLEARY also rented out his botnet for others to use,
12 that is, individuals paid defendant CLEARY money in exchange for
13 being able to conduct DDoS attacks against targets of their
14 choosing using defendant CLEARY's botnet for a certain period of
15 time.
16   iii. Defendant CLEARY assisted LulzSec in its
17 hacking activities, including by identifying security
18 vulnerabilities on victim computers, exploiting such
19 vulnerabilities, conducting DDoS attacks, and also establishing
20 and providing access to servers and other computer resources for
21 LulzSec members to use, including to communicate amongst each
22 other and to store and publish confidential information stolen
23 from LulzSec's victims.
24
25
26
27
28

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 OBJECT OF THE CONSPIRACY

4.   Beginning in or about April 2011, and continuing through in or about June 2011, in Los Angeles County, within the Central District of California, and elsewhere, defendant CLEARY, together with others known and unknown to the Grand Jury, including members of LulzSec, knowingly combined, conspired, and agreed to intentionally cause damage without authorization to a protected computer, in violation of Title 18, United States Code, Section 1030(a)(5)(A).

5.   It was a part and an object of the conspiracy that defendant CLEARY, and others known and unknown to the Grand Jury, including members of LulzSec, knowingly would and did cause the transmission of a program, information, code, and command, and as a result of such conduct, would and did intentionally cause damage without authorization, by impairing the integrity and availability of data, a program, a system, and information on a computer system that was used in and affecting interstate and foreign commerce and communication, causing a loss to one or more persons or entities during a one-year period aggregating at least $5,000 in value.

B.   THE MANNER AND MEANS OF THE CONSPIRACY

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

a.   Defendant CLEARY and other known and unknown co-conspirators, including members of LulzSec, would identify security vulnerabilities in the computer systems of various corporate and government entities for the purpose of causing damage to and/or gaining unauthorized access to such systems.

b.   Taking advantage of the identified security vulnerabilities, defendant CLEARY and other known and unknown co-conspirators, including members of LulzSec, would cause damage to such computer systems.

c.   Defendant CLEARY and other known and unknown co-conspirators, including members of LulzSec, would also hack into such computer systems to obtain confidential information.

d.   Defendant CLEARY would provide LulzSec with access to servers and other computer resources to facilitate communication amongst LulzSec members and to store and publish information stolen from compromised computer systems.

e.   Defendant CLEARY and other known and unknown co-conspirators, including members of LulzSec, would publish the stolen information online.

f.   Defendant CLEARY would instruct an associate who had been contacted by law enforcement about LulzSec to falsely accuse another person of LulzSec's activities.

C.   OVERT ACTS

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

1   Overt Act No. 1:   On or about April 20, 2011, defendant

2   CLEARY and his co-conspirators, including members of LulzSec,

3   hacked into the computer systems of Fox Entertainment Group, Inc.

4   ("Fox"), a commercial broadcasting television company located

5   within the Central District of California, and stole confidential

6   information, including information relating to individuals

7   registered to receive information regarding auditions on

8   "The X-Factor," a Fox television show.

9   Overt Act No. 2:   On or before May 29, 2011, defendant

10 CLEARY and his co-conspirators, including members of LulzSec,

11 hacked into the computer systems of the Public Broadcasting

12 System ("PBS"), a non-profit public television broadcasting

13 service, and defaced the website for the PBS news program "News

14 Hour."

15 Overt Act No. 3:   On or about June 2, 2011, defendant

16 CLEARY and his co-conspirators, including members of LulzSec,

17 hacked into the computer systems of Sony Pictures Entertainment,

18 Inc. ("Sony Pictures"), a major motion picture and television

19 production company located within the Central District of

20 California, and stole confidential information relating to users

21 who had registered on Sony Pictures' website.

22 Overt Act No. 4:   On or about June 2, 2011, defendant

23 CLEARY and his co-conspirators, including members of LulzSec,

24 launched the website lulzsecurity.com.

25 Overt Act No. 5:   On or about June 2, 2011, defendant

26 CLEARY and his co-conspirators, including members of LulzSec,

27 published on lulzsecurity.com information stolen from the

28 computer systems of Fox.

1   Overt Act No. 6:   On or about June 2, 2011, defendant

2 CLEARY and his co-conspirators, including members of LulzSec,

3 published on lulzsecurity.com information stolen from the

4 computer systems of Sony Pictures.

5   Overt Act No. 7:   On or about June 2, 2011, defendant

6 CLEARY provided his co-conspirators, including members of

7 LulzSec, access to computer resources located at QuadraNet, a

8 data and server hosting company in the Central District of

9 California, to facilitate communication between defendant

10 CLEARY's co-conspirators and to store and publish stolen data.

11   Overt Act No. 8:   On or before June 9, 2011, defendant

12 CLEARY provided his co-conspirators, including members of

13 LulzSec, access to computer resources located at GigeNET, a data

14 and server hosting company in Illinois, to facilitate

15 communication between defendant CLEARY's co-conspirators and to

16 store and publish stolen data.

17   Overt Act No. 9:   On or about June 10, 2011, defendant

18 CLEARY instructed an associate who had been contacted by law

19 enforcement regarding LulzSec to provide "disinformation" that

20 "leads away from" LulzSec members; specifically, defendant CLEARY

21 instructed the associate to falsely accuse M.D.M. of LulzSec's

22 activities and offered to provide the associate with fake access

23 logs pointing to M.D.M. to give to law enforcement.

24   Overt Act No. 10:   On or about June 14, 2011, defendant

25 CLEARY launched a DDoS attack against the servers hosting the

26 online game League of Legends, owned and operated by Riot Games,

27 Inc., located within the Central District of California.

28

1   Overt Act No. 11:   On or before June 15, 2011, defendant

2   CLEARY provided his co-conspirators, including members of

3   LulzSec, access to computer resources located at Linode, a data

4   and server hosting company in New Jersey, to facilitate

5   communication between defendant CLEARY's co-conspirators and to

6   store and publish stolen data.

7   Overt Act No. 12:   On or about June 20, 2011, defendant

8   CLEARY launched a DDoS attack against the servers hosting the

9   website of Britain's Serious Organized Crime Agency.

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

1   COUNT TWO

2   [18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I)]

3   8.   The Grand Jury re-alleges and incorporates by reference

4   the allegations set forth in paragraphs one, two, and six of this

5   Indictment.

6   9.   On or about April 21, 2011, in Los Angeles County,

7   within the Central District of California, and elsewhere,

8   defendant CLEARY knowingly caused the transmission of a program,

9   information, code, and command, and as a result of such conduct,

10 intentionally and without authorization caused damage by

11 impairing the integrity and availability of data, a program, a

12 system, and information on a computer system that was used in and

13 affecting interstate and foreign commerce and communication,

14 specifically, the computer systems of Fox Entertainment Group,

15 Inc. ("Fox"), thereby causing a loss to Fox aggregating at least

16 $5,000 in value during a one-year period beginning on or about

17 April 21, 2011.

18

19

20

21

22

23

24

25

26

27

28

1   COUNT THREE

2   [18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I)]
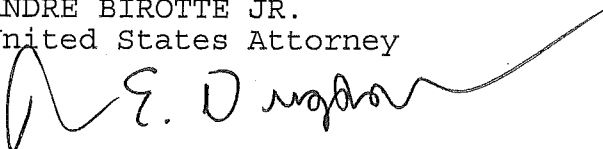
3   10.   The Grand Jury re-alleges and incorporates by reference

4 the allegations set forth in paragraphs one, two, and six of this

5 Indictment.

6   11.   On or about April 30, 2011, in Los Angeles County,

7 within the Central District of California, and elsewhere,

8 defendant CLEARY knowingly caused the transmission of a program,

9 information, code, and command, and as a result of such conduct,

10 intentionally and without authorization caused damage by

11 impairing the integrity and availability of data, a program, a

12 system, and information on a computer system that was used in and

13 affecting interstate and foreign commerce and communication,

14 specifically, DreamHost's computer systems, thereby causing a

15 loss to DreamHost aggregating at least $5,000 in value during a

16 one-year period beginning on or about April 30, 2011.

17   A TRUE BILL

18

19   _/S/_____
                           Foreperson

20 ANDRÉ BIROTTE JR.
   United States Attorney

21

22

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

24

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

26

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

28