

2010 JUL - 8 PM 3: 18  
CLERK U.S. DISTRICT COURT  
CENTRAL DISTRICT OF CALIF.  
LOS ANGELES  
BY \_\_\_\_\_

FILED

UNITED STATES DISTRICT COURT  
FOR THE CENTRAL DISTRICT OF CALIFORNIA

June 2010 Grand Jury

11	UNITED STATES OF AMERICA,	)	Case No. CR 10 00743
12	Plaintiff,	)	<u>I N D I C T M E N T</u>
13	v.	)	[18 U.S.C. § 371: Conspiracy; 18
14	LUIS MIJANGOS,	)	U.S.C. § 1341: Mail Fraud; 18 U.S.C.
15	Defendant.	)	§ 1028A: Aggravated Identity Theft;
16		)	18 U.S.C. §§ 1030(a)(2)(C),
17		)	(c)(2)(B)(ii): Accessing Protected
18		)	Computers to Obtain Information; 18
19		)	U.S.C. § 875(d): Extortion; 18
20		)	U.S.C. §§ 2511(1)(a), (4)(a):
		)	Wiretapping; 18 U.S.C.
		)	§§ 1029(a)(3), (c)(1)(A)(i):
		)	Possession of more than 15
		)	Unauthorized Access Devices; 18
		)	U.S.C. § 2(a), (b): Aiding and
		)	Abetting and Causing an Act to Be
		)	Done]

The Grand Jury charges:

INTRODUCTORY ALLEGATIONS

DEFENDANT LUIS MIJANGOS

1. At all times relevant to this indictment, defendant LUIS MIJANGOS ("defendant MIJANGOS") was an individual residing in Santa Ana, California, within the Central District of California.

MCK:mck

1           2. Defendant MIJANGOS was self-employed as a website  
2 developer and computer consultant in Santa Ana, California, and  
3 accessed the Internet from a dedicated line from his home.

4           3. Defendant MIJANGOS used the following screen names:  
5 gui\_blt, Woods05, CoFfEkId014, ELEvatrHZrD03, Pimpcess03666,  
6 Your3name3here03, Bri23nice, Dmagecntr137, H2IOW14, ELEvATrhRZd03,  
7 Playrgrl137, Your3name3here3, goldlion14, and Hotchit13w.

8           4. Defendant MIJANGOS used the following email accounts:  
9 yousoylammer@hotmail.com, christ@yahoo.com, gui\_blt@live.com,  
10 mistahxxxrightme@aim.com, zapotin@hotmail.com, guich\_x@aim.com,  
11 guicho\_1.1@roadrunner.com, and mijangos3@msn.com.

12 **COMPUTER TERMINOLOGY**

13           Log Files

14           5. Log files are computer-generated lists that contain  
15 various types of information regarding the activities of a  
16 computer. They are often chronological, and record data such as  
17 the time of access to certain records, the processes running on a  
18 computer, and the usage of certain computer resources.

19           Malware

20           6. Malicious software, or "malware," is software that, among  
21 other things, allows malicious computer users to gain remote access  
22 to victim computers without authorization and collect sensitive  
23 information from the computer.

24           Remote Access

25           7. Remote access is the ability to connect to and obtain  
26 control over a computer at a distance, usually over the Internet.

27           Remote Keylogger

28           8. A keylogger is a piece of software or hardware that

1 tracks the keys struck on a keyboard, typically in a covert manner  
2 so that the person using the keyboard is unaware that his/her  
3 actions are being monitored. This allows the subject to learn,  
4 among other things, the victim's passwords to all accounts accessed  
5 by the computer and to read all email and chat transactions by the  
6 victim. A remote keylogger or "remote logger" can be secretly  
7 installed on a computer and can send logfiles of what the keylogger  
8 captured to another computer via the internet.

9 OVERVIEW OF DEFENDANT'S CRIMES

10 9. Beginning on an unknown date and continuing to on or  
11 about June 22, 2010, defendant MIJANGOS and co-schemers throughout  
12 the world engaged in a series of schemes to infect protected  
13 computers throughout the United States. Defendant MIJANGOS and his  
14 co-schemers infected computers in the following manner:

15 a. Defendant MIJANGOS and his co-schemers would develop  
16 or modify existing malware that would cause infected computers,  
17 unbeknownst to the users of the infected computers, to among other  
18 things report to a domain defendant controlled and succumb to  
19 future unauthorized access using other malware.

20 b. Defendant MIJANGOS would install malware on the  
21 compromised computers that gave MIJANGOS remote access, that is,  
22 control over all of the functions of the computer, including  
23 webcams and microphones.

24 c. Defendant MIJANGOS would obtain information from the  
25 compromised computers using a keylogger for use in identity theft,  
26 extortion, and obstruction of justice schemes.

27 10. Defendant MIJANGOS would access the compromised computers  
28 to further a variety of criminal ends:

1 a. Defendant MIJANGOS and his co-schemers would use  
2 keyloggers on the compromised computers to obtain confidential  
3 authentication information, including credit card numbers and bank  
4 account numbers. Defendant MIJANGOS would then use that  
5 information to engage in credit card fraud.

6 b. Defendant MIJANGOS would obtain intimate images and  
7 videos of women and teenage girls from the victim computers without  
8 the authorization of the owners of those images and videos.  
9 Defendant MIJANGOS would then contact the victim women and girls  
10 and threaten to post those intimate images and videos on the  
11 Internet unless they provided him with additional intimate images  
12 and videos.

13 c. Using victim computers belonging to teenage boys,  
14 defendant MIJANGOS would impersonate those teenage boys and trick  
15 their girlfriends into providing him with intimate images and  
16 videos. Defendant MIJANGOS would then contact the victim women and  
17 girls and threaten to post those intimate images and videos on the  
18 Internet unless they provided him with additional intimate images  
19 and videos.

20 d. To perpetuate the scheme, and to avoid law  
21 enforcement detection, defendant MIJANGOS would activate the  
22 webcams and microphones on victim computers, as well as review the  
23 keyloggers installed on the victim computers, to determine whether  
24 the human victims had contacted law enforcement or notified friends  
25 or family about the scheme.

COUNT ONE

[18 U.S.C. § 371]

11. The Grand Jury repeats and re-alleges paragraphs 1 through 10 of this Indictment as if fully set forth herein.

THE OBJECTS OF THE CONSPIRACY

12. Beginning on a date unknown to the Grand Jury and continuing through on or about March 10, 2010, in Orange County, within the Central District of California, and elsewhere, defendant MIJANGOS, together with co-conspirators known and unknown to the Grand Jury, knowingly combined, conspired, and agreed to commit the following offenses against the United States:

a. To commit mail fraud, in violation of Title 18, United States Code, Section 1341; and

b. To commit access device fraud, in violation of Title 18, United States Code Section 1029(a)(2).

THE MANNER AND MEANS OF THE CONSPIRACY

13. The objects of the conspiracy were carried out, and to be carried out, in substance, as follows:

a. Defendant MIJANGOS and his co-conspirators would develop or modify existing malware that would cause infected computers, unbeknownst to the users of the infected computers, to among other things report to a domain defendant controlled and succumb to future unauthorized access using other malware.

b. Defendant MIJANGOS and his co-conspirators would install malware on the compromised computers that allowed defendant and his co-conspirators control over all of the functions of the computer, including webcams and microphones.

c. Defendant MIJANGOS and his co-conspirators would

1 obtain information from the compromised computers for use in  
2 identity theft schemes.

3 OVERT ACTS

4 14. In furtherance of the conspiracy, and to accomplish its  
5 objects, defendant MIJANGOS, together with co-conspirators known  
6 and unknown to the Grand Jury, committed and willfully caused  
7 others to commit the following overt acts, among others, in the  
8 Central District of California and elsewhere:

9 Overt Act No. 1: On or about November 26, 2008, a co-  
10 conspirator using the screen name "Manhattan" sent personal  
11 identifying information regarding victim J.E. to defendant  
12 MIJANGOS.

13 Overt Act No. 2: On or about January 2, 2009, defendant  
14 MIJANGOS ordered a credit card in the name of J.E.

15 Overt Act No. 3: On or about March 20, 2009, defendant  
16 MIJANGOS and a co-conspirator using the screen name "Demonio666vip"  
17 discussed how to test malware to make it undetectable by popular  
18 anti-virus programs.

19 Overt Act No. 4: On or about March 31, 2009, defendant  
20 MIJANGOS and a co-conspirator using the screen name "Manhattan"  
21 obtained credit information without authorization regarding certain  
22 individuals.

23 Overt Act No. 5: On or about March 31, 2009, defendant  
24 MIJANGOS and a co-conspirator using the screen name "Manhattan"  
25 discussed obtaining a false passport.

26 Overt Act No. 6: On or about April 10, 2009, a co-  
27 conspirator using the screen name "Manhattan" sent defendant  
28 MIJANGOS stolen credit card information, along with victim names

1 and addresses.

2 Overt Act No. 7: On or about April 10, 2009, defendant  
3 MIJANGOS and a co-conspirator using the screen name "Manhattan"  
4 discussed credit card information stolen earlier that day.

5 Overt Act No. 8: On or about April 10, 2009, defendant  
6 MIJANGOS and a co-conspirator using the screen name "Manhattan"  
7 discussed the relative merits of using Western Union or American  
8 Express to transfer the proceeds of credit card fraud.

9 Overt Act No. 9: On or about April 10, 2009, defendant  
10 MIJANGOS told a co-conspirator using the screen name "Manhattan"  
11 that he could only process five fraudulent credit cards a day, not  
12 10 or twelve as "Manhattan" proposed.

13 Overt Act No. 10: On or about April 13, 2009, defendant  
14 MIJANGOS and a co-conspirator using the screen name "Manhattan"  
15 made a fraudulent purchase over PayPal and deleted the confirmation  
16 email to hide the transaction.

17 Overt Act No. 11: On or about May 12, 2009, a co-conspirator  
18 using the screen name "Manhattan" sent defendant MIJANGOS  
19 unauthorized access devices, including names, addresses, credit  
20 card numbers, and email addresses.

21 Overt Act No. 12: On or about May 12, 2009, defendant  
22 MIJANGOS and a co-conspirator using the screen name "Manhattan"  
23 discussed the use of unauthorized access devices, including names,  
24 addresses, credit card numbers, and email addresses.

25 Overt Act No. 13: On or about May 12, 2009, defendant  
26 MIJANGOS and a co-conspirator using the screen name "Manhattan"  
27 discussed the transfer of the proceeds of credit card fraud.

28 Overt Act No. 14: On or about September 18, 2009, a co-

1 conspirator using the name "mauricio garza arcos" ordered t-shirts  
2 from Design by Humans using a stolen credit card number and  
3 statikgto@gmail.com as a contact email address.

4 Overt Act No. 15: On or about October 8, 2009, a co-  
5 conspirator using the name "mauricio garza arcos" ordered t-shirts  
6 from Design by Humans using a stolen credit card number and  
7 statikgto@gmail.com as a contact email address.

8 Overt Act No. 16: On or about November 13, 2009, defendant  
9 MIJANGOS ordered t-shirts from Design by Humans using a stolen  
10 credit card number and used statikgto@gmail.com as a contact email  
11 address.

12 Overt Act No. 17: On or about November 14, 2009, a co-  
13 conspirator using the name "St4tlk // Money Buster Team" provided  
14 sent defendant MIJANGOS stolen credit card information, along with  
15 victim names and addresses.

COUNT TWO

[18 U.S.C. §§ 1341, 2(b)]

15. The Grand Jury repeats and re-alleges paragraphs 1 through 10 of this Indictment as if fully set forth herein.

16. Beginning on an unknown date, and continuing through on or about March 10, 2010, in Orange County, within the Central District of California, and elsewhere, defendant MIJANGOS, together with others known and unknown to the Grand Jury, knowingly and with intent to defraud, devised, participated in, and executed a scheme to defraud Wachovia Bank as to material matters, and to obtain money and property from Wachovia Bank and others by means of material false and fraudulent pretenses, representations, and promises, and the concealment of material facts.

17. Specifically, on or about January 5, 2009, defendant MIJANGOS, for the purpose of executing and attempting to execute the above-described scheme to defraud, willfully caused an envelope containing an unauthorized credit card in the name of victim J.B.E. to be placed in an authorized depository for mail matter to be sent and delivered by the United States Postal Service, according to the directions thereon, to Santa Ana, California, within the Central District of California.

COUNT THREE

[18 U.S.C. § 1028A]

1  
2  
3 18. The Grand Jury repeats and re-alleges paragraphs 1  
4 through 10 of this Indictment as if fully set forth herein.

5 19. On or about January 5, 2009, in Orange County, within the  
6 Central District of California, and elsewhere, defendant MIJANGOS,  
7 together with others known and unknown to the Grand Jury, knowingly  
8 transferred, possessed, and used, without lawful authority, a means  
9 of identification of another person, that is, the name of J.E.,  
10 during and in relation to mail fraud, a felony violation of Title  
11 18, United States Code, Section 1341, as charged in Count Two,  
12 above.

## COUNTS FOUR THROUGH ELEVEN

[18 U.S.C. §§ 1030(a)(2)(C), (c)(2)(B)(ii); §§ 2(a), (b)]

20. The Grand Jury repeats and re-alleges paragraphs 1 through 10 of this Indictment as if fully set forth herein.

21. On or about the following dates, defendant MIJANGOS, using a computer in Santa Ana, California, intentionally accessed and caused to be accessed computers used in interstate and foreign commerce, without authorization and in excess of authorized access, and obtained and caused to be obtained information from those computer to further criminal and tortious acts:

COUNT	DATE	UNAUTHORIZED ACCESS
FOUR	3/28/2009	Accessed computer belonging to D.D. without authorization and in excess of authorization to obtain information on A.V. used to intentionally inflict emotional distress
FIVE	4/10/2009	Accessed computer belonging to D.D. without authorization and in excess of authorization to obtain information used to extort C.G. in violation of California Penal Code Section 523 and intentionally inflict emotional distress
SIX	4/13/2009	Accessed computer belonging to S.G. without authorization and in excess of authorization to obtain information used to extort S.G. in violation of California Penal Code Section 523 and intentionally inflict emotional distress
SEVEN	4/18/2009	Accessed computer belonging to L.W. without authorization and in excess of authorization to obtain information used to intentionally inflict emotional distress
EIGHT	11/4/2009	Accessed computer without authorization and in excess of authorization to obtain information used to intentionally inflict emotional distress on G.M.

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

COUNT	DATE	UNAUTHORIZED ACCESS
NINE	12/24/2009	Accessed computer belonging to M.L.T. without authorization and in excess of authorization to obtain information used to videotape M.L.T. surreptitiously in violation of California Penal Code Sections 647(j) (2) and (3)
TEN	2/8/2010	Accessed computer belonging to S.G. without authorization and in excess of authorization to obtain information used to defraud S.G. in violation of Title 18, United States Code, Sections 1344 and 1029(a) (2)
ELEVEN	2/11/2010	Accessed computer belonging to A.M. without authorization and in excess of authorization to obtain information used to intentionally inflict emotional distress

COUNT TWELVE

[18 U.S.C. § 875(d)]

22. The Grand Jury repeats and re-alleges paragraphs 1 through 10 of this Indictment as if fully set forth herein.

23. On or about August 14, 2008, in the Central District of California, and elsewhere, defendant LUIS MIJANGOS, knowingly and willfully, and with the intent to extort money and other thing of value, did transmit in interstate and foreign commerce from Santa Ana, California, to Puyallup, Washington, an email communication to victim K.S., and the email communication contained a true threat to injure the reputation of K.S.

COUNTS THIRTEEN AND FOURTEEN

[18 U.S.C. §§ 2511(1)(a) and (4)(a)]

24. The Grand Jury repeats and re-alleges paragraphs 1 through 10 of this Indictment as if fully set forth herein.

25. On or about the following dates, in Orange County, within the Central District of California, and elsewhere, defendant MIJANGOS, intentionally intercepted the contents of the following oral communications:

COUNT	DATE	COMMUNICATION
THIRTEEN	4/7/2009	Communication belonging to D.D.
FOURTEEN	2/3/2010	Communication belonging to S.S.

COUNT FIFTEEN

[18 U.S.C. §§ 1029(a)(3), (c)(1)(A)(i)]

26. The Grand Jury repeats and re-alleges paragraphs 1 through 10 of this Indictment as if fully set forth herein.

27. On or about March 10, 2010, in Orange County, within the Central District of California, defendant LUIS MIJANGOS, knowingly and with intent to defraud, possessed at least fifteen unauthorized access devices as defined in Title 18, United States Code, Section 1029(e)(1) and (3), namely, bank account usernames and passwords, checking account routing and account numbers, credit card account and verification/security numbers, check card account numbers, and Social Security numbers, with said possession affecting interstate and foreign commerce.

COUNT SIXTEEN

[18 U.S.C. § 1028A]

28. The Grand Jury repeats and re-alleges paragraphs 1 through 10 of this Indictment as if fully set forth herein.

29. On or about March 10, 2010, in Orange County, within the Central District of California, defendant LUIS MIJANGOS knowingly transferred, possessed, and used, without lawful authority, a means of identification of another person, that is, the name of C.G., during and in relation to Access Device Fraud, a felony violation

///

///

///

1 of Title 18, United States Code, Section 1029(a)(3), as charged in  
2 Count Fifteen of this indictment.  
3

4 A TRUE BILL

5  
6 15/  
FOREPERSON

7  
8 ANDRÉ BIROTTE JR.  
United States Attorney

9 *Christine C. Ewell*

10  
11 CHRISTINE C. EWELL  
Assistant United States Attorney  
Chief, Criminal Division

12  
13 WESLEY L. HSU  
Assistant United States Attorney  
Chief, Cyber and Intellectual Property Crimes Section

14  
15 MARK C. KRAUSE  
Assistant United States Attorney  
Deputy Chief, Cyber and Intellectual Property Crimes Section  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28