Approved: _____
MARK F. MENDELSOHN
Assistant United States Attorney

Before: HONORABLE RONALD L. ELLIS
United States Magistrate Judge
Southern District of New York

- x

UNITED STATES OF AMERICA	:	TO BE FILED UNDER SEAL
	:	
	:	COMPLAINT
- v. -		
	:	Violations of
ADRIAN LAMO,		18 U.S.C.
	:	§§ 1030(a)(5)(A)(ii) and 1029(a)(2)
	:	
		COUNTY OF OFFENSE:
Defendant.	:	New York

- x

SOUTHERN DISTRICT OF NEW YORK, ss.:

CHRISTINE A. HOWARD, being duly sworn, deposes and says that she is a Special Agent of the Federal Bureau of Investigation and charges as follows:

COUNT ONE

1. From in or about February 2002 through in or about April 2002, in the Southern District of New York and elsewhere, ADRIAN LAMO, the defendant, intentionally accessed a protected computer without authorization and, as a result of such conduct, recklessly caused damage to 1 and more persons during a 1-year period aggregating at least $5,000 in value, to wit, LAMO, without the knowledge or authorization of the New York Times Co., Inc. (the "New York Times"), repeatedly accessed the New York Times' private intranet, and altered the contents of New York Times databases including a database containing the personal information of contributors to the New York Times' Op-Ed page, and by such conduct caused a loss resulting in damage

to the New York Times in excess of $25,000 during a one-year period.

(Title 18, United States Code, Section 1030(a)(5)(A)(ii).)

COUNT TWO

2. From in or about February 2002 through in or about April 2002, in the Southern District of New York and elsewhere, ADRIAN LAMO, the defendant, knowingly and with intent to defraud trafficked in and used one and more unauthorized access devices during a one-year period, and by such conduct obtained anything of value aggregating $1,000 and more during that period, to wit, LAMO created, and subsequently used, approximately five user identification names and passwords under the New York Times' account with the electronic information service LexisNexis, and by such conduct obtained LexisNexis search services valued in excess of $300,000 during a one-year period.

(Title 18, United States Code, Section 1029(a)(2).)

The bases for the deponent's knowledge and the foregoing charges are, in part, as follows:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") assigned to the Cybercrime Task Force of the FBI's New York Field Division. I have been so employed for approximately two years, and have been an agent of the FBI for approximately six and one-half years. In addition, I have an undergraduate degree in computer science. In the course of my career with the FBI, I have participated in the investigation and prosecution of numerous crimes involving unauthorized access of protected computers.

2. I have participated in the investigation of this matter, and I am familiar with the information contained in this affidavit based on my own personal participation in the investigation, my review of documents and computer records, and conversations I have had with other law enforcement agents and other individuals. Because this affidavit is submitted for the limited purpose of establishing probable cause to arrest ADRIAN LAMO, the defendant, I have not included herein the details of every aspect of the investigation. Where the actions, conversations, and statements of others are related herein, they are related in substance and in part, except where otherwise

indicated.

3. Through my training and experience as an FBI agent, I am familiar with "hackers" and "hacking." In general, hackers discover and explore vulnerabilities and security weaknesses in computer networks and software. Hackers carry out their activities using hacker tools that can either be custom written software code or, as is more common, software readily available for download on the internet or for purchase.

The New York Times Intrusion

4. In or about late February 2002, I read an article on website SecurityFocus.com dated February 26, 2002 and entitled "New York Times Internal Network Hacked" (the "Article"). The Article reported that ADRIAN LAMO, the defendant, had hacked into the New York Times' private intranet[1] (the "NYT Intranet") and accessed, among other things, a database containing personal information (including home telephone numbers and Social Security numbers) for over 3,000 contributors to the New York Times' Op-Ed page. The Article further stated that LAMO had altered that database by adding a record for "Adrian Lamo" along with such personal information as his cellular telephone number and email address, and listing his expertise as "computer hacking, national security, communications intelligence." According to the Article, LAMO admitted to the author of the Article in the course of an interview that LAMO was responsible for the New York Times intrusion. LAMO also described in detail how he had gained access to the system through a proxy server[2]; and detailed additional conduct undertaken while inside the NYT Intranet.

5. In or about late February 2002, I contacted an employee of The New York Times ("NYT Representative One") regarding the intrusion described in the Article. NYT Representative One informed me of the following, among other

[1] An intranet is a computer network belonging to an organization, usually a corporation, accessible only by the organization's members, employees, or others with authorization.

[2] A "server" generally is a computer or device on a network that manages network resources; for example, a file server is a computer storage device dedicated to storing files. A "proxy server" is a server that sits between a client application, such as a web browser (*i.e.*, Netscape, Internet Explorer) and a server. Proxy servers have two main purposes: (1) to improve network performance; and (2) to filter requests.

things:

(a) On February 26, 2002 -- prior to the publication of the Article later that day -- the author of the Article contacted NYT Representative One and stated that ADRIAN LAMO, the defendant, had gained access to the NYT Intranet; that LAMO was able to download the Social Security numbers of New York Times employees and personal information regarding 3,000 contributors to the New York Times Op-Ed page; that LAMO had accessed information regarding New York Times home delivery subscribers; and that LAMO had gained this access to the NYT Intranet through an open proxy server. The author of the Article provided the Internet Protocol addresses[3] ("IP addresses") for seven proxy servers allegedly accessed by LAMO. The author of the Article stated that his source, *i.e.* LAMO, had provided screen captures[4] showing internal images of the NYT Intranet, along with other information confirming the intrusion. **The author of the Article also provided LAMO's cellular telephone number —- (415) 505-HACK[5] -- to NYT Representative One.**

(b) Following the initial conversation with the author of the Article, the New York Times conducted an internal investigation into the alleged intrusion and confirmed that an unauthorized intruder had accessed the NYT Intranet using a proxy server[6] that was among the seven identified by the author of the Article.[7] The investigation revealed that the intruder

---

[3] An Internet Protocal or IP address is a unique numeric address use by computers on the Internet to communicate.

[4] A "screen capture" is an electronic image, something like a digital snapshot, of an individual's computer screen at a particular moment in time.

[5] I have obtained and reviewed subscriber and billing records from the cellular telephone company that provides service to telephone number (415) 505-HACK. Those records reflect that the telephone is subscribed to by an individual with the last name Lamo, with a mailing address in northern California. Based on my research using various databases including ChoicePoint, a provider of identification and credential verification services to the government, I have determined that the individual at that billing address is believe to be the father of ADRIAN LAMO, the defendant. In addition, LAMO maintains a website at http://adrian.adrian.org. On that website, LAMO lists his telephone number as (415) 505-HACK.

[6] A representative of the New York Times has advised me that this proxy server is located in Manhattan.

[7] Based on my training and experience, I have learned

had
accessed a New York Times staff list; obtained the name and Social Security number of a former New York Times employee; and using that information logged onto the NYT Intranet as a "superuser" -- that is, a user with full administrative rights to access and make changes to the network. Using that superuser access, the intruder created another superuser account under the fictitious user name "Eric Yee." The intruder then used the Eric Yee superuser account to access various sites within the NYT Intranet, including an administrative database of contact information for various public sources (the "administrative database") and a database containing personal information and Social Security numbers for contributors to the New York Times Op-Ed page (the "Op-Ed database"). NYT Representative One advised me that the intruder had altered the Op-Ed database, adding a record for "Adrian Lamo" and personal information such as Lamo's cellular telephone number (*i.e.*, (415) 505-HACK) and email address, and listing his expertise as "computer hacking, national security, communications intelligence." NYT Representative One also advised me that a similar record for "Adrian Lamo" had been added to the administrative database.

6. In or about late May 2002, another representative of the New York Times ("NYT Representative Two") advised me that in or about May 2002, LexisNexis (an online subscription service that provides legal, news, public records and business information for a fee) had contacted the New York Times to report unusually high levels of activity associated with a number of the userids/passwords assigned to the New York Times' user account with LexisNexis (the "compromised userids/passwords"). NYT Representative Two told me that the New York Times had subsequently conducted an internal investigation to determine who was responsible for the unusual activity. That investigation, including analysis of electronic logs relating to the NYT Intranet, revealed that each of the compromised userids/passwords was created by the account of the fictitious user Eric Yee that the intruder had created during the course of the unauthorized intrusion into the NYT Intranet.

---

that a software tool called "Proxy Hunter" is widely used by hackers to identify unsecured proxy servers on the internet. In connection with a different computer intrusion of MCI WorldCom, discussed below in paragraph 15, it has been reported in the press that ADRIAN LAMO, the defendant, used Proxy Hunter to identify an unsecure proxy server, which he then used to access MCI WorldCom's internal network.

7. Representatives of The New York Times have provided me with copies of the following records pertaining to the intrusion, among others:

(a) the New York Times administrative database (admin_db) and the Op-Ed database (Oped_db) as they existed prior to the intrusion;

(b) the New York Times administrative database (admin_db) and the Op-Ed database (Oped_db) as they existed after the intrusion;

(c) log files[8] from the proxy server accessed by the intruder;

(d) log files from various other servers on the NYT Intranet;

(e) an email automatically generated by the New York Times' computer network when a new user identification is created reflecting that the Eric Yee user identification was created on February 20, 2002 at 8:10 p.m. EST; and

(f) the user identification numbers/passwords ("userids/passwords") associated with five LexisNexis accounts created by the fictitious Eric Yee user account.

8. I have analyzed the materials provided by the New York Times described in paragraph 7 above and, based on that analysis and conversations with various New York Times personnel, have determined the following:

(a) New York Times server logs reflect that an intruder had compromised the NYT Intranet at least as early as February 14, 2002.

(b) Between on or about February 14, 2002 and on or about February 26, 2002, New York Times Intranet server logs reflect that an intruder repeatedly accessed the New York Times Intranet through a New York Times proxy server and queried various directories on the servers, modified news stories saved on the server, and modified various databases.

(c) an email automatically generated on February 20, 2002

[8] Log files lists actions that have occurred in connection with a computer server. For example, Web servers maintain log files listing every request made to the server.

at 8:10 p.m. EST by the New York Times computer network with the subject "Change in stafflist" reflects that at that date and time the intruder, using the superuser account of a former New York Times employee, created a new superuser account under the fictitious name Eric Yee.

(d) New York Times server logs reflect that on February 20, 2002 at 9:30 p.m. EST the intruder logged on using the newly created Eric Yee superuser account and then proceeded to add a record to a New York Times administrative database under the name "Adrian Lamo."

(e) New York Times server logs reflect that on February 20, 2002, at 10:41 p.m. EST the intruder, still logged into the Eric Yee superuser account, added a record for "Adrian Lamo" to the New York Times Op-Ed database, a database of biographical and other personal information regarding contributors to the Op-Ed page.

9. A representative of the New York Times had advised me that the New York Times has spent in excess of $25,000 confirming, assessing, and repairing the damage caused by the computer intrusion described herein.

10. In or about early June 2002, I spoke with a representative of LexisNexis (the "LexisNexis Representative") on a number of occasions. The LexisNexis Representative advised me that five userids/passwords under the New York Times' account with LexisNexis had been used to conduct more than 3,000 searches over a period of three months. The five userids were TOOMANYSECRETS, PROTAGONIST, LOCUST, VAISHNAV and NU1UJB. The LexisNexis representative also advised me that during the month of February 2002, the searches conducted by these five userids/passwords represented approximately 18% of all searches performed under the New York Times account. The LexisNexis Representative advised me that he had communicated with the New York Times about the activity under the compromised userids/passwords and confirmed that the userids/passwords were created using the fictitious Eric Yee user account. The LexisNexis Representative advised me that these userids/passwords had been used to access LexisNexis services from, among other places, IP addresses associated with two Kinko's locations, one in Oxnard, California and one in Sacramento Valley, California.[9] The LexisNexis Representative

[9] In a number of articles published by reporters who have interviewed LAMO, it is reported that LAMO carried out many of his computer intrusions from his laptop at a Kinko's

further advised me that the charges incurred through the use of the five compromised userids/passwords amounted to approximately $300,000.

11. The LexisNexis Representative provided me with copies of the log files pertaining to userids TOOMANYSECRETS, PROTAGONIST, LOCUST, VAISHNAV, and NU1UJB, including the following information: (a) date and time stamp; (b) IP address that accessed the userid; (c) the query entered; (d) the LexisNexis database searched; (e) the type of search; and (f) how the account was accessed, *e.g.* through the internet or through a network such as the New York Times' Intranet.

12. I have reviewed the LexisNexis log files identified above and based on that review and my conversations with LexisNexis personnel have determined the following:

(a) searches were performed in various different LexisNexis libraries for the following, among other queries:

1. "Adrian Lamo";

1. various other individuals who have the last name "Lamo" or who, based on my research using various databases including ChoicePoint, formerly had the last name "Lamo";

I. an address in California that, based on my research using various databases including ChoicePoint, appears to be the home address of the parents of ADRIAN LAMO, the defendant, and is the same address as the billing address for cellular telephone number (415) 505-HACK;

I. other addresses on the same street as the above address;

1. names of various reputed hackers;

1. executives of America On-Line ("AOL"); and

1. various individuals believed to be associated with ADRIAN LAMO, the defendant, in the hacking community.

(b) on February 26, 2002 (the same date

---

location.

that the author of the Article first notified the New York Times that its network had been compromised by ADRIAN LAMO, the defendant), in a four minute period queries were made in the LexisNexis NEWS library[10] for:

(1) "NEW YORK TIMES HACKER";

(2) "HACKER AND DATE GEQ 02/26/2002";[11] and

(3) "ADRIAN LAMO."

(c) LexisNexis searches using the unauthorized accounts were performed as late as March 20, 2002.

13. In the course of my investigation I have read various articles regarding the New York Times hack, including the following:

(a) An article published on February 26, 2002 on the website SecurityFocus.com reported that ADRIAN LAMO, the defendant, admitted having accessed the New York Times internal network through a proxy server and viewing, among other things, a database of employees' names and Social Security numbers. According to the article, LAMO is reported to have stated that with respect to the New York Times intrusion, "The very first server I looked at was running an open proxy." LAMO continued: "The server practically approached me." In explaining how he went about obtaining access to the New York Times intranet, LAMO is reported to have stated that "[t]he proxy was on a different network, dealing with the management of subscription information, but it was trusted by their internal network." Regarding the employee database that LAMO accessed from within the New York Times Intranet, LAMO stated that "[f]rom what I have been able to tell, it was a backup database being used for

[10] The LexisNexis NEWS library contains stories from newspapers, magazines, wire services, transcripts and newsletters.

[11] This query called for a search for all news articles dated February 2, 2002 that included the term "hacker."

research."

(b) An article published on February 26, 2002 in Newsbytes (a Washington Post web site) reported that ADRIAN LAMO, the defendant, acknowledged responsibility for the computer intrusion of the New York Times, and that Newsbytes had reviewed screen captures that depicted the New York Times' "Everyone, Everywhere" newsroom contact database.

(c) An article published on February 27, 2002 by website Computerworld.com reported that ADRIAN LAMO, the defendant, acknowledged responsibility for the computer intrusion of the New York Times and that with respect to adding a record under the name "Adrian Lamo" in a New York Times database, LAMO stated: "It was more of a whim than anything else." LAMO added that "[i]t just came naturally to me while I was there."

(d) An article published on February 27, 2002 by MSNBC.com reported that ADRIAN LAMO, the defendant, had provided MSNBC.com with screen captures that showed what appeared to be databases from the NYT Intranet.

(e) An article published on February 27, 2002 by the Associated Press reported that ADRIAN LAMO, the defendant, had acknowledged responsibility for the New York Times hack, and that LAMO had stated that he had first obtained access to the NYT Intranet ten days before notifying the New York Times.

Other Computer Intrusions By ADRIAN LAMO, The Defendant

14. During the course of my investigation of the New York Times hack, I have searched public information available on-line for further information regarding ADRIAN LAMO, the defendant, including further information about other computer intrusions for which LAMO has acknowledged responsibility in interviews with members of the press. As a result of my research, I have obtained and reviewed articles

and videos from various on-line and print publications in which LAMO was interviewed by the authors and claimed responsibility for various computer intrusions and related activities. I have also spoken and corresponded with representatives of the companies that were hacked. In the case of each computer intrusion identified below, LAMO has (a) admitted to a member of the press his responsibility for the intrusion, as reported in a published article or video, (b) described his methods of intrusion and compromise, and (c) in some instances, also personally admitted his responsibility to representatives of the victim company and provided corroboration that he was in fact the intruder:

(a) Excite@Home - In or about May 2001, ADRIAN LAMO, the defendant, gained unauthorized access to Excite@home's internal computer network.

(b) Yahoo! - In or about September 2001, ADRIAN LAMO, the defendant, gained unauthorized access to Yahoo's website through a proxy server and altered several news stories.

(c) Microsoft - In or about October 2001, ADRIAN LAMO, the defendant, gained unauthorized access into a customer database on Microsoft's internal network.

(d) MCI WorldCom - In or about November 2001, ADRIAN LAMO, the defendant, gained unauthorized access to MCI WorldCom's internal computer network through a MCI WorldCom proxy server.

(e) SBC Ameritech - In or about December 2001, ADRIAN LAMO, the defendant, gained unauthorized access to SBC Ameritech's internal computer network, including access to customer information.

(f) Cingular - In or about May 2003, ADRIAN LAMO, the defendant, gained unauthorized access to the computer system of a company that

issues insurance to Cingular customers, including access to Cingular customer information.

15. In a April 16, 2003, an article was published in a newspaper called the San Francisco Weekly entitled "A Duty To Hack," which quoted ADRIAN LAMO, the defendant, extensively. In the article, the reporter states that LAMO is preparing to announce his biggest hack to date. According to the reporter, LAMO defined his target on the record as a "critical-infrastructure-related company" (quotes in original article). LAMO goes on to state: "In terms of my personal sense of the intrusion and what it affects, I see this as more epic than anything I've worked on in the past . . . There's a sense of rightness about it. I believe it's broader in scope, but it also has more potential to go terribly south."

WHEREFORE, deponent prays that ADRIAN LAMO, the defendant, be arrested and imprisoned or bailed as the case may be.

_____
CHRISTINE A. HOWARD
Special Agent
Federal Bureau of Investigation

Sworn to before me this
__ day of August 2003

_____
UNITED STATES MAGISTRATE JUDGE