AFFIDAVIT IN SUPPORT OF COMPLAINT

I, Peter Garza, having been duly sworn, hereby depose and state:

1. I am an "investigative or law enforcement officer of the United States" within the meaning of Title 18, United States Code, Section 2510(7), that is, I am an officer of the United States empowered to conduct investigations of offenses enumerated in Title 18, United States Code, Section 2516, under the circumstances provided herein. I am a Special Agent with the Naval Criminal Investigative Service (NCIS), assigned to the NCIS Field Office in Los Angeles, California. NCIS is empowered by law, among other things, to investigate all violations of federal law committed against the Department of Defense. I have been a Special Agent with NCIS for approximately 6 years. I am currently assigned as the Computer Crimes Coordinator for the NCIS Field Office in Los Angeles. During my employment as a special agent with NCIS I have worked on numerous criminal investigations involving the use and misuse of computers that required the application of my training and experience in computer forensics. My investigative training includes:

a. A computer forensics course conducted by the International Association of Computer Investigative Specialists (November, 1991);

b. Participation in the Telecommunications Fraud Training program conducted by the Federal Law Enforcement Training Center (August, 1992);

c. A course in computer evidence analysis conducted by

the Federal Law Enforcement Training Center (March, 1994); and,

d. A Novell Network Technologies course taught by Computer Focus of Oxnard, California (February, 1995).

2. I am familiar with, and have participated in, all of the traditional methods of investigations, including, but not limited to, electronic surveillance, visual surveillance, general questioning of witnesses, use of the grand jury, use of search warrants, use of confidential informants, use of pen register and trap and trace devices, and the use of undercover agents.

3. This affidavit is submitted in support of an application for a complaint against Julio Cesar Ardita ("Ardita"). As detailed below, there is probable cause to believe that Ardita has committed the following offenses:

a. Fraudulent possession of unauthorized computer passwords, user identification names, codes and other access devices[1], in violation of Title 18, United States Code, Section 1029 (a)(3);[2]

b. Fraudulent and destructive activity in connection with computers, in violation of Title 18, United States Code,

---

[1] An "access device" is defined in Title 18, United States Code, Section 1029(e)(1) to include "any ...code, account number, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services or any thing of value..."

[2] Pursuant to Title 18, United States Code, Section 1029(a)(3), it is a felony to "knowingly and with intent to defraud possess[] fifteen or more devices which are . . . unauthorized access devices."

Section 1030(a)(5);[3] and

c. Illegal interception of electronic communications, in violation of Title 18, United States Code, Section 2511(1)(a).

4. I am familiar with all aspects of this investigation, and the circumstances surrounding the facts and the offenses described in this affidavit. I make this affidavit, in part, on personal knowledge based on my participation in this investigation and, in part, upon information and belief. I have personally interviewed personnel who manage or assist in the management of most of the computer systems discussed in this affidavit and reviewed records from their computer systems made available to me. In addition, I have received information through oral and written reports about this and other investigations from agents and computer experts employed by NCIS, the Federal Bureau of Investigation (in cooperation with which this investigation is being conducted) and NASA's Office of Inspector General. Since this affidavit is being submitted for the limited purpose of seeking a complaint against Julio Cesar Ardita, I have not set forth each and every fact

---

[3] Pursuant to Title 18, United States Code, Section 1030(a)(5), it is unlawful for a person, "through means of a computer used in interstate commerce or communications, knowingly [to] cause the transmission of a program, information, code or command to a computer system if - (i) the person causing the transmission intends that such a transmission will - (I) damage, or cause damage to, a computer, computer system, network, information, data or program; [and] . . . (ii) the transmission of the harmful component of the program, information, code or command - (I) occurred without [] authorization . . . and (II) (aa) causes loss or damage to one or more other persons of value aggregating $1,000 or more during any 1-year period."

learned in the course of the investigation.

INTRODUCTION

Background

5. The investigation resulting in this criminal complaint had three phases which, for clarity, will be followed in this affidavit. During the initial phase, a then unknown intruder (referred to in this affidavit initially as "the Intruder") was discovered to be making unauthorized use of accounts on the computer system administered by the Faculty of Arts and Sciences at Harvard University, Cambridge, Massachusetts and using these accounts without authorization to access and to attempt to access other computer systems connected to Harvard's through the Internet. A computer, such as Harvard's, accessible by means of the Internet, is known as a "host computer." [4] Accordingly, the system administered by the Harvard Faculty of Arts and Sciences frequently will be referred to in this affidavit as the "FAS Harvard host."

6. Because the Intruder was accessing the FAS Harvard host through a widely known modem bank and other Internet hosts and because he was making unauthorized use of the accounts through which he was accessing the FAS Harvard host and other Internet hosts (effectively using the legitimate account holders' identities as his aliases or covers), it was not possible initially to determine the Intruder's true identity.

7. Nonetheless, it was possible to distinguish the Intruder

---

[4] A glossary containing specialized terms used in this Affidavit is appended.

from other users of the FAS Harvard host and the Internet through his repetition of certain conduct when using the FAS Harvard host. This identifying behavior, detailed below, involved (1) use of programs with unique names, (2) to obtain account names and associated passwords through the unlawful interceptions of electronic communications, (3) on overlapping groups of host computer systems.

8. During the second phase of the investigation, the Naval Criminal Investigative Service and the Federal Bureau of Investigation obtained court authorization to conduct electronic surveillance of the Intruder's communications to and from the FAS Harvard host. These communications were identified and isolated by a monitoring computer which was triggered by the tell-tale use of accounts which the Intruder had compromised, communications from Internet host computers from which the Intruder was accessing the FAS Harvard host, communications to Internet host computers which the Intruder was attacking from the FAS Harvard host, and the use of unique files and programs which the Intruder utilized when engaged in his unlawful activities.

9. During the course of the electronic surveillance, the Intruder was monitored referring to himself by the moniker "griton," which is Spanish for "screamer." He also was repeatedly observed accessing the FAS Harvard host from four computer systems in Buenos Aires, Argentina.

10. During the third, and final phase, the Intruder - then located in Buenos Aires, Argentina, and known by his moniker

"griton" - was identified as Julio Cesar Ardita. As detailed in ¶¶ 71-76 below, this identification was accomplished primarily through the examination of previous activity of "griton" on a computer bulletin board, the contents of which were accessible on the Internet, and the analysis of records, in the United States and Argentina.

Offenses Committed by Ardita

11. While many computer systems allow guest privileges for certain functions, most, including those referred to in this affidavit, require an individual to have an authorized account on the system to have access to particular programs and files on that system. Insofar as they can be used alone or in conjunction with other access devices to obtain services, information and other things of value, the account names or numbers and associated passwords or codes are access devices within the definition of Title 18, United States Code, Section 1029(e)(1).

12. There is probable cause to believe, for reasons detailed below, that Ardita has obtained numerous account/password combinations on the FAS Harvard host without authorization and used those accounts to obtain and attempt to obtain without authorization account/password combinations on other systems connected to the FAS Harvard host through the Internet. The possession of fifteen or more unauthorized account/password combinations (access devices, as defined) knowingly, and with intent to defraud, is a violation of Title 18 U.S.C. § 1029(a)(3).

13. Ardita was able to obtain account password combinations

through "sniffer" programs which he transmitted to host computers at victim sites.[5] A sniffer program intercepts electronic communications over the system on which it is placed containing account/password combinations and stores them for later recovery. As each of the attacked, host computers was connected to host computers in other states and countries through the Internet, and thus affected interstate and foreign commerce, there is probable cause to believe Ardita's unlawful interception of electronic communications through the planted sniffer programs violated Title 18, United States Code, Section 2511(1). Further, the transmission in conjunction with the sniffer programs of camouflaging programs, which destroyed records otherwise kept on the victim host computers, evidenced probable violations of Title 18, United States Code, Section 1030(a)(5). [6]

Harm Caused by the Intrusions

14. As described below, a number of the host computers to which the Intruder gained unauthorized access are affiliated with the Department of Defense. The Department of Defense network hosts which have been compromised by Ardita reside in networks which contain sensitive and proprietary, although not classified,

---

[5] It has not been possible, so far, to determine whether Ardita downloaded any files from the victim computers.

[6] 1030(a)(5) requires as a jurisdictional prerequisite that the loss or damage to one or more persons aggregate $1000 or more during a one year period. One of the agencies into which Ardita gained unauthorized access and destroyed information and data to conceal that access, has estimated that it cost in excess of $100,000 to investigate the intrusions from the FAS Harvard host during the periods Ardita was active and to reconfigure its systems in response to those intrusions.

government information. These networks store information related to U.S. Department of the Navy and NASA research programs and contain files relating to research on state-of-the-art satellites, radiation and energy related engineering. Ardita's unauthorized access to the Department of Defense network hosts potentially gave him the ability to steal and transfer these results and files.[7]

15. Ardita's unauthorized access to these systems, and the use to which Ardita made of this access, put the violated network hosts, themselves, at risk of harm, as well. Ardita used programs to obtain broad and powerful access on network hosts he had broken into, known as "root" access. Root access allowed Ardita to alter programs to conceal his activity and could enable him to alter, erase or destroy files on the network. In addition, by gaining root access and running sniffer programs, Ardita could intentionally or accidently cause the network hosts to erase files or become inaccessible to the legitimate users of the network.

16. These actual and potential harms are not limited to the known, violated hosts described in this affidavit. Because the "sniffer" programs which Ardita installed on the targeted network hosts enabled Ardita to obtain additional user identifications and passwords and thus to gain access to additional network hosts, other as yet unidentified network hosts have been and will be equally at risk of theft of proprietary information and harm.

---

[7] The cost of isolating an intrusion and reconfiguring a system to protect its files after an intrusion can readily cost tens of thousands of dollars in lost productivity of the system's administrators and users, and lost access to the system during the reconfiguration process.

Initial Identification of the Intruder Through His Pattern of Unlawful Activity

17. Host computers, i.e., computers accessible by means of the Internet, are identified by an electronic address, known as an internet host name. For example, the host computer administered by the Harvard Faculty of Arts and Sciences at Harvard is named fas.harvard.edu. The host's given name is "fas"; "harvard" identifies the location of the host; and "edu" identifies the owner of the system as an educational system.

18. All electronic communications transmitted across networks of computers are transmitted in "packets." The information to be communicated is broken down into small units. Each unit, or packet, contains the address of the sending computer, the address of the receiving computer, and some portion of the message or data being communicated. These packets are dispersed throughout the network, each finding its own way to the receiving computer. Upon arrival, the packets are reassembled into a coherent message or data file. Consequently, the host computer that sends an electronic communication usually can be identified by the receiver.

19. Beginning by approximately July 12, 1995, host computers in several states and in Mexico and the United Kingdom reported unauthorized attempts to intrude, and successful intrusions, originating from fas.harvard.edu, the FAS Harvard host.

The Beginning of the Intrusion Investigation

20. This investigation began after an intrusion was detected into a computer network operated by the Naval Command, Control and Ocean Surveillance Center ("NCCOSC"). NCCOSC is a unit of the

United States Navy located in, among other places, San Diego, California. NCCOSC maintains several computer networks which, in order to communicate with each other and with other computer networks around the world, are accessible by means of the Internet.

21. I have spoken with Ronald Broersma, Corporate Network Administrator, NCCOSC San Diego, and with Lieutenant Commander (LCDR) Dean Rich, assigned to the Fleet Information Warfare Center, Norfolk, Virginia. LCDR Rich is a recognized expert in information security. His academic background includes a Master in Science degree in Computer Science from the Naval Postgraduate School, Monterey, California. The corporate network administrator, LCDR Rich and I each reviewed the victim computer networks at NCCOSC and the audit logs associated with these computers. These discussions and reviews revealed the following.

22. On August 25, 1995, an individual using the user identification "chult" accessed the NCCOSC computer host named mindy.nosc.mil. "Chult"[8] accessed mindy.nosc.mil from the FAS Harvard host. "Chult" installed several files onto mindy.nosc.mil.[9] Included in the files installed by "chult" was a program referred to in the industry as a "sniffer" program, a program used frequently by computer intruders to capture packets containing user

---

[8] Most Internet computers use the UNIX operating system, which is case sensitive. The case sensitivity will be respected throughout this affidavit except at the beginning of sentences, where the first letter will be capitalized to conform with normal grammatical form.

[9] A directory of network hosts referred to in this Affidavit is appended.

identification and associated passwords for network access. The sniffer program actually intercepts electronic communications as they are transmitted over the network and then stores a selected portion of each communication. In this case, the sniffer program installed by "chult" was designed to store the first 256 bytes of the communications, which often include the user's account name and password. "Chult" named this program "sni256."

23. The "sni256" program installed by "chult" created a file named "test." This file served as the repository for the illegally intercepted user names and passwords. "Chult" also installed a program named "zap." Most Internet host computers use the UNIX operating system. UNIX, in turn, has a utility program named "who" which is used to identify other users currently logged into the network. Information pertaining to users on a UNIX host, used by the "who" utility, is stored on the UNIX host and a continuously-updated log is created. The "zap" program installed by "chult" deleted references to his access in the "who" log. "Chult" also installed a program named "pinga" which, upon review, has been confirmed to obtain "root," or unlimited, access on the compromised network host. With "root" access, the user has the authority to view, alter and install files anywhere on the network host. Such access generally is limited to system administrators.

24. "Chult" was a legitimate user identification which actually belongs to a NCCOSC system administrator. However, this NCCOSC system administrator did not install the programs on August 25 and did not direct or authorize anyone to use his account to do

so.

25. The Intruder from FAS Harvard host repeatedly accessed mindy.nosc.mil using the user name "chult" on August 25, 1995. During one session, the Intruder used mindy.nosc.mil to access another network host named dax.nosc.mil which is the network host for another NCCOSC computer system located in Arlington, Virginia. While accessing dax.nosc.mil, the Intruder installed his "sni256," "test" and "zap" programs and files.

26. The placement of unauthorized files and programs on mindy.nosc.mil was discovered by a NCCOSC system administrator on August 28, 1995. On August 29, 1995, a more comprehensive audit program was activated on mindy.nosc.mil.

27. On August 29, 1995, the Intruder logged into mindy.nosc.mil as "chult" from FAS Harvard host. Specifically, Broersma related that computer records for the NCCOSC network indicate a connection was established by an intruder from FAS Harvard host on August 29, 1995. These records show that an intruder from FAS Harvard host logged into a user account called "chult" on the NCCOSC host known as mindy.nosc.mil. Broersma said the Intruder executed commands to determine who was on the network and then executed the "zap" program to remove records concerning his own access. The Intruder then copied the contents of his "test" file, containing illegally obtained user names and passwords, to his terminal. The Intruder then deleted the contents of the "test" file and restarted the illegal wiretap program, "sni256."

28. Broersma also related that he had detected no intrusion into the NCCOSC network from FAS Harvard host before the intrusion into the host known as irc.nosc.mil, which occurred on or about August 24, 1995. This host also contained the signature "sni256," "test" and "zap" programs and files which had been installed on August 24, 1995. According to Broersma's records, the original connection to mindy.nosc.mil at NCCOSC appears to have occurred via the "chult" user account on irc.nosc.mil, on or before August 25, 1995.

29. On September 4, 1995, the Intruder also used his mindy.nosc.mil connection to access another NCCOSC network host, at the Naval Command Control and Ocean Surveillance Center at San Diego, California, named fountainhead.nosc.mil. Because the Intruder accessed a user name other than "chult" after using "chult" to access the results of the sniffer file installed on mindy.nosc.mil, it is my opinion, based upon my training and experience, that the Intruder used a new account name obtained from his sniffer file on mindy.nosc.mil to give him access to fountainhead.nosc.mil.

30. On September 19, 1995, I spoke with Special Agent Deborah Rocco of the Naval Criminal Investigative Service, who informed me of an interview which she had conducted earlier that day with Darryl Cleveland, the System Manager of the Army Research Lab ("ARL") in Edgewood, Maryland. Darryl Cleveland informed Special Agent Rocco that an intruder from FAS Harvard host had attempted to gain unauthorized access to one of the host computers on ARL's

computer network on or about August 12, 1995, between 4:16 p.m. and 4:19 p.m. Darryl Cleveland related that the attempt appeared to have been unsuccessful. Darryl Cleveland could not pinpoint the user account on FAS Harvard host from which the intrusions had originated.

31. On September 20, 1995, I spoke with Special Agent Gary Walker of the Navy Criminal Investigative Service, who informed me of an interview which he had conducted on September 19, 1995 with the system manager of the Army Research Lab in Aberdeen, Maryland. The system manager informed Agent Walker that an intruder from FAS Harvard host had made approximately ninety attempts to gain unauthorized access to different branches of the ARL's computer network, at different locations throughout the United States. According to the system manager, these attempts took place from August 12, 1995 until August 16, 1995 and appeared to have been unsuccessful. The system manager could not pinpoint the user account on FAS Harvard host from which the intrusions had originated.

32. On October 11, 1995, I spoke with the systems manager for the Electrical Engineering Department of the California Institute of Technology in Pasadena, California ("Caltech"). He explained that on October 4, 1995, he discovered a "sniffer" program called "sni256" was running on a Caltech network host computer known as scrooge.systems.caltech.edu. It was located in a hidden subdirectory called "..." which also contained files called "test" and "zap". As described in this affidavit, "sni256," "test" and

"zap" are signature files used by the Intruder. The systems manager also stated that on the following day, October 5, 1995, the Caltech network host was probed unsuccessfully twice from FAS Harvard host.

Efforts to Identify and Localize the Intruder Within the FAS Harvard host

33. During the latter part of August, September and October, extensive efforts were undertaken to localize and identify the Intruder. Those efforts evidenced defining behaviors including:

(a) The Intruder was accessing and attempting to access without authorization an overlapping set of government and education network hosts from several different accounts at FAS Harvard host; and

(b) The Intruder, once he had obtained unauthorized access to other network hosts, had created files and implanted programs with unique names in a number of those hosts.

34. As summarized herein, the Intruder repeatedly had used changing accounts of the FAS Harvard host to gain unauthorized access to an overlapping group of victim networks. Once on many of the victim networks, the Intruder had installed similar files with identical names, performing similar functions. These files were peculiar to the performance of unauthorized functions associated with "hackers,"[10] in that they enabled the Intruder to gain unauthorized access to accounts on the victim computers and to

[10] A "hacker" is a slang term frequently used to refer to a person who breaks into computer systems with wrongful intent.

conceal the intrusions themselves from system managers who might otherwise detect the intrusions through routine audits of the computer logs. The unique names of the files utilized by the Intruder included "sni256," "test,"[11] "zap," "pinga," "ropt," "roption," "HotterThanMojaveInMyHeart," and "InfamousAngel."[12] Searches of the archives on the Internet have not revealed files performing the same unauthorized functions to have been published on the Internet under the names "sni256," "test," "zap," or "pinga." Further, a check with Special Agent Jolene Smith Jameson at the National Computer Crime Squad, FBI Washington Metropolitan Field Office, Washington, D.C., has revealed that none of these file names have been associated with other groups or individuals involved with "hacker" activity.[13]

35. On September 8, 1995, I spoke with Ron Holland, Networking and Computer Security Group with NASA's Jet Propulsion Laboratory, Pasadena, California. Holland related that he found files similar to those which had been described as being installed by the Intruder at the NCCOSC network. Holland checked a subdirectory called "/bin" on merlin.jpl.nasa.gov and found the file called "pinga". Mr. Holland said systems administrators

---

[11] As his unlawful activity continued, "sni256" would be abbreviated as "sni" and "test" would be abbreviated as "tst."

[12] The Intruder created for his files and programs a subdirectory with a unique name, as well, "...".

[13] The file names "ropt," "roption," "HotterThanMojaveIn MyHeart," and "InfamousAngel" have been found to be used by at least one other group, which has made them publicly available over the Internet.

examined this file and it was found to be written to exploit system vulnerabilities and obtain "root" privileges on this host computer. Holland also found a hidden subdirectory named "..." (that is, three dots) which contained files named "sni256," "test" and "zap." Holland confirmed that the "sni256" file was a program that first intercepted users' identification and password commands to the host -- [illegible] examined and was found to delete records used by the UNIX "who" program on this host computer; the" zap" file on the JPL/NASA hosts was similar to the "zap" program installed on the NCCOSC network host computers, specifically mindy.nosc.mil and dax.nosc.mil.

36. On September 14, 1995, I spoke with Special Agent Thomas Gilchrist, NCIS Los Angeles Field Office, who related that he had re-interviewed Holland, who provided additional information regarding the Intruder's activity. Review of information provided by Mr. Holland confirmed a FAS Harvard host user identified as "margolin" obtained unauthorized access to the "debabani" account on the JPL/NASA network host called merlin.jpl.nasa.gov on or about September 8th. Before or during that session, the file "sni256" had been installed on the system. This unauthorized connection to merlin.jpl.nasa.gov originated from FAS Harvard host.

37. During subsequent discussions and electronic mail communications with Ed Chan, who is the Ames Network Security Manager responsible for ssa1.arc.nasa.gov, I learned that on September 8, 1995, a user from FAS Harvard host connected to an

account with a user identification of "yuen" on an Ames network host known as ssa1.arc.nasa.gov. Mr. Chan told me that he had contacted the authorized user of the account, and the authorized user had reported finding an unfamiliar file named "ropt" in his home directory.[14] Mr. Chan related that examination of the "ropt" file revealed that when executed, it attempted to exploit a known vulnerability in the UNIX operating system to obtain root privileges on the host computer. Root privileges enable a user to control the host computer, allowing the user to run programs such as the sniffer programs found on previous compromised hosts.

38. Mr. Chan's review of the "ropt" file indicated that the file executed commands contained in two files named "HotterThanMojaveInMyHeart" and "InfamousAngel." The script file looked for these files in a subdirectory called "/tmp." The "/tmp" subdirectory is a standard subdirectory in UNIX for temporary files which are deleted if the UNIX computer is restarted. Mr. Chan related the records which were available for the sa1.arc.nasa.gov host indicate that the "ropt" script file and the "HotterThanMojaveInMyHeart" and "InfamousAngel" files in the "/tmp" subdirectory were used in the attempt to gain root privileges with a technique that exploits a known vulnerability in UNIX systems.

39. On September 20, 1995, I spoke with Special Agent Gary Walker, NCIS, Dahlgren, Virginia, who related the following

---

[14] A home directory is a user's assigned work space on the host computer and enables the user to store his own computer files and programs.