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 computers and then recorded the intercepted information to another file called "test." Holland said the file called "zap" had been 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.

information he received from Randy Taylor, Network Engineer, Naval Research Laboratory (NRL), Washington, DC.

40. On August 6, 1995, a user from FAS Harvard host successfully gained access to an account named "guest" on a host called i7140rr.itd.nrl.navy.mil and later logged in again on this host to a user account named "wang." Taylor related the account named "shuang" was being used at FAS Harvard host to access the NRL network. Once the "shuang" user from FAS Harvard host gained access to a valid account on i7140rr.itd.nrl.navy.mil, the 42 other network host computers on this network would allow connections using the "wang" account. A search of the computer hosts on this network revealed the file called "pinga" on the hosts known as i7140rr.itd.nrl.navy.mil and abyss.itd.nrl.navy.mil at NRL. This file was used by the "shuang" intruder to obtain root access to i7140rr.itd.nrl.navy.mil on August 7, 1995 and to obtain root access on abyss.itd.nrl.navy.mil on September 11, 1995. In addition the "shuang" intruder created a subdirectory called "..." in the "/usr/etc/" subdirectory, where he installed a file called iss13.jue. This iss13.jue file is a publicly available computer security scanning program which scans a UNIX computer for security vulnerabilities.

41. During my earlier discussions with Broersma he had related a similar file called "pinga," used to obtain root access, was found on mindy.nosc.mil and dax.nosc.mil. Broersma had also described the use of a subdirectory called "..." on mindy.nosc.mil and dax.nosc.mil, where the Intruder attempted to hide files he had

installed on the compromised systems.

42. On September 18, 1995, I contacted a system administrator at the Centro de Computo Academico, Departamento de Fisica, Universidad de Sonora (Academic Computing Center, Physics Department, University of Sonora), Hermosillo, Sonora, Mexico. The system administrator related that on August 25, 1995, computer logs for network host fisica.uson.mx at the University of Sonora Mexico showed that, earlier that day, an unauthorized user had logged into a user account named "garibay" from FAS Harvard host. The system administrator related that the Intruder from FAS Harvard host installed a script file called "roption" in the "garibay" user's home directory on fisica.uson.mx. The "roption" file contained instructions to use the files "HotterThanMojaveInMyHeart" and "InfamousAngel," located in a subdirectory called "/tmp," to gain root access on fisica.uson.mx using the above described vulnerability.

43. In my conversations with the administrators for the network hosts which have been compromised, I have been told that there are no legitimate users which are known to use a host at Harvard University. None of the people responsible for compromised hosts at the arc.nasa.gov, jpl.nasa.gov, and the nosc.mil domains have reported that there are users who would have had legitimate connections from FAS Harvard host.

44. On October 16, 1995, I interviewed the systems manager, Mathematics and Statistics Department, University of Massachusetts ("UMASS"), Amherst, Massachusetts ("the UMASS system manager"),

regarding computer intrusions into the UMASS network host known as comet.phast.umass.edu. The UMASS systems manager related he had been informed by NASA's Ames Research Center ("ARC"), Moffett Field, California on September 18, 1995 that an account named "yuen," on the ARC host named ssa1.arc.nasa.gov, had been accessed by an unknown intruder. The UMASS systems manager was informed that the UMASS network may have been compromised because Yuen also had an account on a UMASS network host computer and the Ames Research Center's network had been probed from UMASS.

45. The UMASS systems manager said that his computer logs reflected that someone had gained unauthorized access to comet.phast.umass.edu. and had installed the files "pinga," "sni256," and "zap" on August 29, 1995 at approximately 23:40. The logs further showed that the "sni256" sniffer file was activated on October 10, 1995, when the unauthorized user gained access to the computer after establishing a telnet connection from an internet network host in Texas. This file again was activated on October 12, 1995, at approximately 00:58, when the intruder used the telnet protocol to connect to comet.phast.umass.edu from the FAS Harvard host, where the intruder was logged in under the user account called "margolin."

46. The UMASS systems manager discovered and terminated the "sni256" file on October 12, 1995. The UMASS systems manager then copied the file called "test" which had been created by the "sni256" program and removed the "test" file from comet.phast.umass.edu. On October 14, 1995, the intruder connected

from the "margolin" account on the FAS Harvard host and ran the "pinga" program and logged out.

47. The UMASS system manager stated that the computer system logs for comet.phast.umass.edu also evidenced that an unauthorized user logged into the "rmillang" account from the "margolin" account on the FAS Harvard host. After discovering this, the UMASS systems manager reviewed the ".history" file information for the user "rmillang" The UNIX operating system creates a file called ".history" (the word history preceded by a dot) in a user's home directory which maintains a running log of a certain number of commands issued by a user. The UMASS systems manager stated that his review of the ".history" file information for the user account called "rmillang" shows the intruder logged in, ran the identifying program "pinga," and then logged out.

48. The UMASS systems manager explained the legitimate user of the "rmillang" account is a first year graduate student in the UMASS Mathematics and Statistics department. He regularly accesses his account during the day, and is not known to access his account during the late night hours. The UMASS systems manager's review of the comet.phast.umass.edu system's logs, which record all logins, did not reveal any record of a login to the "rmillang" account during the times the Intruder connected with comet.phast.umass.edu from the FAS Harvard host, or, in fact, from June 10, 1995 to October 1995. The UMASS systems manager stated that he knows the legitimate "rmillang" user did regularly access his account on comet.phast.umass.edu during that period. The UMASS systems

manager opined that the Intruder used the "zap" program which deleted not only the Intruder's sessions, but all sessions when the "rmillang" account was accessed from the computer system's records up through October 1995.

Real-Time Monitoring of the Intruder's Activities in November and December, 1995

49. Based on the probable cause established in the initial phase of the investigation, the United States applied for and obtained court authorization to conduct electronic surveillance of the Intruder's electronic communications to and from the FAS Harvard host. The orders further directed Harvard University to furnish the FBI and NCIS with the information, facilities and technical assistance necessary to accomplish the interceptions unobtrusively and with a minimum of interference to the persons whose communications might be intercepted. As a result of these court authorized interceptions, the government was able to locate the city from which the Intruder appeared to be accessing the Internet and to partially identify the Intruder through a unique moniker he had given himself. The Intruder - "griton" - was accessing the Internet initially from Buenos Aires, Argentina.

50. A network monitoring program was obtained from the Automated Systems Security Incident Support Team (ASSIST), Defense Information Systems Agency, Washington, DC, and was used to aid in the interceptions and to minimize the interception of electronic communications other than those evidencing the Intruder's criminal activity. The network monitoring program was designed to monitor packets of information transmitted across a network and can be

configured to store selected, captured packets for later review. Once stored, the captured data can be searched for particular words, phrases or other information (called "text-strings") and the packets containing these strings can be reassembled to reconstruct the network sessions in which they were created. These reconstructed sessions can then be replayed to a computer monitor to depict the timing and combination of "keystrokes" typed during the selected session, or the captured session can be copied to a text file.

51. The network monitoring program was installed on a computer located on the network connection between the FAS Harvard host and the router at the Harvard University Faculty of Arts and Sciences Computer Center ("the FAS Harvard router"). It was configured to monitor all transmissions between the FAS Harvard host and FAS Harvard router, searching for one of a limited set of file and account names and computer addresses typed by the user and associated with the Intruder. The file and account names and computer addresses which the network monitoring program was set up to detect included the names of accounts and addresses of Internet hosts which the Intruder was believed to have compromised, as well as certain commands he was believed to have executed and the names of files he was believed to have installed at sites to which he had gained unauthorized access from FAS Harvard host.

52. Communications across the network link between the FAS Harvard host and FAS Harvard router are transmitted at up to ten megabits per second, that is 10,000,000 ones or zeroes which form

pieces of information, per second. While the monitoring program executed its detection function, communications flowed continuously through the computer's RAM, or short-term, memory. The network monitoring program did not capture, display or permanently store the communications which it monitored.

53. Once the network monitoring program detected an occurrence of one of the targeted file names and words, it displayed and recorded a text-string (particular words, phrases or other information) of up to approximately eighty characters identifying the context in which the target word or command was intercepted. At the same time, it isolated and recorded the computer session of the user who typed in the text-string until the user terminated his connection to the FAS Harvard host.

54. The government initially sought to distinguish, and thus avoid review of, any session by anyone other than the Intruder by examining the logged text-string context of the triggering file name, which was automatically recorded as discussed above. The only sessions examined by law enforcement agents were those sessions where the displayed text-string or a secondary scan by computer utility programs for key words strongly indicated evidence of unlawful activity by the Intruder.

55. On November 20, 1995, the text string "/usr/bin/pinga" was detected by the network monitoring program. This text string indicated that the "pinga" program used by the Intruder was executed via the FAS network. Accordingly, I extracted this and related data streams (electronic communications one direction or

the other between the FAS Harvard host and FAS Harvard router) which made up communications believed to be the Intruder's into a readable text form. Review of the transcript of these data streams revealed that the Intruder established a connection to the FAS Harvard host from the Internet host with the Internet protocol address of 200.3.40.17, which belongs to an Internet host known as clirisc.telecom.com.ar registered to Telecom Argentina, Buenos Aires, Argentina, and then established a connection from the FAS Harvard host during this session to the Internet protocol address of 134.75.138.3. This address is registered to the System Engineering Research Institute ("SERI"), Seoul, Republic of Korea. When the Intruder connected to the FAS Harvard host from Telecom Argentina and accessed SERI in Seoul, the Intruder executed programs known to have been used by the Intruder on several computer systems described earlier in the affidavit. While logged into SERI in Seoul the Intruder executed the "pinga" program to obtain control of the computer system, ran "zap" to conceal that he was logged in under the account name of "wgchoe," and copied the "test" file, which contained the results of a previously installed sniffer program, named "sni", which captured, among other information, user identifications and passwords.[15] The sniffer program believed to be used by the Intruder in past intrusions was called "sni256"; it appears that the Intruder chose to shorten the name of the program to "sni."

---

[15] On this occasion, the Intruder copied approximately 31 user identification and password combinations which had been intercepted by the sniffer program.

56. Ten data streams[16] believed to be associated with the Intruder were intercepted on November 22, 1995. The word which triggered interception of each of these ten data streams was again "pinga" embedded in the text string "/usr/bin/pinga." The text string indicated that the "pinga" program, described earlier in my affidavit as a program known to be used by the Intruder, was executed via the FAS Harvard host. Accordingly, I extracted these data streams into readable text form.

57. The transcript of the November 22, 1995 data streams revealed that the Intruder again established a connection to the FAS Harvard host from the Internet protocol address of 200.3.40.17, which belongs to an Internet network host known as clirisc.telecom.com.ar, registered to Telecom Argentina in Buenos Aires, Argentina. During this session into the FAS Harvard host, the Intruder established connections to the Internet network hosts known as venus.fisica.unlp.edu.ar, which is registered to Universidad de La Plata, La Plata, Argentina; splinter.coe.neu.edu, which is registered to Northeastern University, in Boston, Massachusetts; and orac.wes.army.mil, which is registered to the

---

[16] The number of data streams intercepted is very likely to overstate the number of computer sessions which were intercepted because of the manner in which the triggering mechanism of the network monitoring software works. For example, when the Intruder, as described below, sent an electronic communication from one Internet host through the FAS Harvard host to a third Internet host, the network monitoring software saw this as up to four electronic data streams or communications - one from the Intruder into the FAS Harvard host, one from the FAS Harvard host out to the third Internet host, and two complementary streams if the third host responded through the FAS Harvard host to the Intruder - rather than a single computer session.

U.S. Army Engineer Waterways Experimentation Stations, in Vicksburg, Mississippi.

58. The transcript of these connections revealed that the Intruder executed the same programs for illegally intercepting computer passwords and for disguising his presence which he had previously used in other computer networks, as detailed earlier in my affidavit. Specifically, the Intruder executed the "pinga" program to obtain control of each of the computer systems which he accessed from the FAS Harvard host. He also executed a command to list the contents of a subdirectory named "..." (three dots), which contained the files "sni," "test," and "zap." While logged into compromised accounts on each of the three target sites, the Intruder searched the "test" file, which contained the passwords and user identifications captured by the previously installed sniffer program named "sni." After searching the contents of the "test" file, the Intruder copied the contents to his terminal. The Intruder then re-started the sniffer program to capture further user identifications and passwords. Before logging off, the Intruder ran "zap" to conceal the account names he was using on each of the targeted systems.[17]

59. Review of the data streams for the Intruder's session on November 22, 1995, confirmed the Intruder retrieved user

[17] The captured data streams nonetheless enabled us to identify the accounts he was using on each of the targeted systems. On venus.fisica.unlp.edu.ar the Intruder accessed an account named "torres." On splinter.coe.neu.edu the Intruder accessed the account "arambel." On orac.wes.army.mil the Intruder accessed an account named "lichvar."

identification and passwords which had been intercepted on venus.fisica.unlp.edu.ar, splinter.coe.neu.edu, and orac.wes.army.mil by the sniffer programs planted in them. On the Internet host known as venus.fisica.unlp.edu.ar the Intruder copied approximately fourteen user account and password combinations which had been intercepted and stored in the "test" file. On the Internet host named splinter.coe.neu.edu the Intruder copied the output of the "test" file which contained approximately fourteen user identification and password combinations, in addition to the user account he used to access splinter.coe.neu.edu. While connected to the Internet host known as orac.wes.army.mil the Intruder copied approximately nine user identification and passwords which had been intercepted by the sniffer program and stored in a file called "test."

60. Computer logs containing connection information for the Intruder on the FAS Harvard host revealed that on November 20 and November 22, 1995, the Intruder accessed an account named "qrr2" on the FAS Harvard host from the Internet host with the Internet protocol address of 200.3.40.17 (clirisc.telecom.com.ar registered to Telecom Argentina). Comparison of the intercepted data streams with this login information indicated that the Intruder used this "qrr2" account during the sessions intercepted by the network monitoring software on those dates.[18]

---

[18] Computer logs containing connection information for the Intruder on the FAS Harvard host revealed the Intruder logged into the FAS Harvard host under the user account "qrr2" on December 19, 1995, as well, during a period when the monitoring system had been shut down temporarily. During this session the

200.9.112.137, which is registered under the name tapera.bf.epm.br and is also at the Escola Pualistade Medicina, was listed by the iss program as using an older version of electronic mail software which has known, but correctable, vulnerabilities.

65. On December 6, 1995, the Intruder executed the program named "ropt," which exploits a vulnerability in some versions of the UNIX operating system to obtain access to an Internet host as a "root" user. Network monitoring software triggered on the target word "roption" which is embedded in the "ropt" program and captured a series of data streams which indicated that the Intruder logged into the FAS Harvard host from an Internet network host named ts1-e0.starnet.net.ar with the IP address of 200.26.3.18. While logged into the FAS Harvard host from the ts1-e0.starnet.net.ar host, the Intruder had established a connection to an Internet network host with the IP address of 200.9.151.173 under the account name of "operador." This host is registered with the host name of chiloe.chilepac.com which is on a network operated by a company known as Chilepac S.A. in Santiago, Chile.

66. While the Intruder was logged into the chiloe.chilepac.com host the Intruder viewed the file containing the computer program called "ropt." I saw that the instructions in this program referred to program files called "HotterThanMojaveInMyHeart" and "InfamousAngel" which were to be written to a subdirectory called "/tmp." This "/tmp" sub-directory is a standard area where certain versions of the UNIX operating system store temporary files which are deleted if the system is re-

200.9.112.137, which is registered under the name tapera.bf.epm.br and is also at the Escola Pualistade Medicina, was listed by the iss program as using an older version of electronic mail software which has known, but correctable, vulnerabilities.

65. On December 6, 1995, the Intruder executed the program named "ropt," which exploits a vulnerability in some versions of the UNIX operating system to obtain access to an Internet host as a "root" user. Network monitoring software triggered on the target word "roption" which is embedded in the "ropt" program and captured a series of data streams which indicated that the Intruder logged into the FAS Harvard host from an Internet network host named ts1-e0.starnet.net.ar with the IP address of 200.26.3.18. While logged into the FAS Harvard host from the ts1-e0.starnet.net.ar host, the Intruder had established a connection to an Internet network host with the IP address of 200.9.151.173 under the account name of "operador." This host is registered with the host name of chiloe.chilepac.com which is on a network operated by a company known as Chilepac S.A. in Santiago, Chile.

66. While the Intruder was logged into the chiloe.chilepac.com host the Intruder viewed the file containing the computer program called "ropt." I saw that the instructions in this program referred to program files called "HotterThanMojaveInMyHeart" and "InfamousAngel" which were to be written to a subdirectory called "/tmp." This "/tmp" sub-directory is a standard area where certain versions of the UNIX operating system store temporary files which are deleted if the system is re-

started. Both "HotterThanMojaveInMyHeart" and "Infamous Angel" have been associated with the Intruder in the past, as detailed earlier in my affidavit. The Intruder executed the "ropt" program in an unsuccessful attempt to gain access to a host with the IP address of 151.10.81.10, using the user name "NolInParticular." The Intruder then executed the "ropt" program, unsuccessfully targeting a host named ciro.chilepac.com, again using user name "NolInParticular." The Intruder continued attempts to gain access to the following Internet hosts with the "ropt" program under the user name of "NolInParticular:" palborno.chilepac.com, with the IP address of 200.9.151.131; aklenner.chilepac.com, with the IP address of 200.9.151.171; ealbornoz.chilepac.com, with the IP address of 200.9.151.144 and a host with the IP address of 140.115.45.105 on a network registered to the Ministry of Education Computer Center Taipei, Taiwan, Republic of China. In reviewing the Intruder's activity on chiloe.chilepac.com, I saw that he viewed, installed and edited a program called "mailscript." As he was editing "mailscript," the program displayed an explanation that it exploits a flaw in a particular version of sendmail software on computers using the UNIX operating system in order to obtain root access. The Intruder also appeared to have installed the files called "sni" and "zap," with which he has been associated repeatedly in the past.

67. While logged into the chiloe.chilepac.com host the Intruder also established a telnet connection to an Internet host with the IP address of 200.9.151.160, with the host name of

gte.chilepac.com, and logged in under the user name of "operador". While on gte.chilepac.com, the Intruder viewed the contents of the password file for this host and a file which lists all hosts on its network. The Intruder then disconnected from gte.chilepac.com and listed the contents of a subdirectory called "..." (three dots) on the chiloe.chilepac.com hosts. This "..." subdirectory contained the files called "sni," "tst" and "zap." Just as the Intruder appears to have shortened the name of his sniffer file from "sni256" to "sni," he appears to have shortened the name of his output file from "test" to "tst." The Intruder viewed the contents of the "tst," which contained portions of sessions intercepted by the "sni" program on chiloe.chilepac.com.

68. Later in the same session, the Intruder used the telnet protocol to connect from the FAS Harvard host to the host with the IP address of 140.115.45.105 at the Ministry of Education Computer Center, Taipei, Taiwan, R.O.C, where he logged into the account named "sm5002." There, the Intruder executed the program called "pinga," to obtain root privileges, and ran the program called "zap," to conceal the account name he was using. The Intruder viewed the contents of the subdirectory called "..." and viewed the path for the current working directory, which was "/home1/5002/..."

69. Another set of data streams intercepted on December 6, 1995, documented a session when the Intruder logged into Internet Relay Chat ("IRC") under the nick-name of "griton" and joined a channel called "#hack.br." IRC allows users to engage in communications over the Internet in the interactive nature of a

conversation, rather than sending stored communications such as electronic mail to each other. It is the practice on IRC to assign yourself a nickname when you log onto an IRC server (an Internet host computer which is linked to a worldwide network of IRC servers to facilitate the "chat" sessions). Communications take place over channels which are either public - for all to see and join in if they wish - or private - open only to invited participants. Based on my training and experience, I am aware that computer intruders, commonly referred to as "hackers," use public IRC channels to "advertise" that they are active and then invoke the "private" message facility in IRC to exchange interactive messages directly. During those interactive messages, users can communicate and also transfer files.

70. Later in the evening of December 6, 1995, an additional session for the Intruder was intercepted by the monitoring computer. Data streams for this session indicate the Intruder logged into the FAS Harvard host from the IP address of 200.3.40.17, which is a host on a network operated by Telecom Argentina, Buenos Aires, Argentina. While logged into the FAS Harvard host the Intruder established a connection to a host with the IP address of 200.9.151.173, which is chiloe.chilepac.com. While on chiloe.chilepac.com, the Intruder executed the "pinga" program and then changed to a sub-directory called "...," where he executed the "zap" program to conceal that he was logged into the account named "operador." The Intruder then accessed IRC and joined a channel called "#argentina" under the nick-name of

"griton."

Identification of "Griton," the Intruder, in Buenos Aires, Argentina

71. "Griton" has now been identified as Julio Cesar Ardita through two independent means. First, "griton" made several descriptive postings on a computer bulletin board known as "yabbs," including an open invitation to visit his own computer bulletin board in Buenos Aires. The location of griton's computer bulletin board has been traced by the Argentine Federal Police to Ardita's residence in Buenos Aires. Second, Telecom Argentina has confirmed that the Intruder into the FAS Harvard host from their computer system, in turn, had broken into their system from a telephone number located at Ardita's residence.

72. A search of files accessible to the public through the Internet disclosed that "griton" previously had posted a number of communications on a computer bulletin board known as "yabbs." On a computer bulletin board, a user can post messages accessible to all other users of the bulletin board service, just as an individual might tack a note to a cork bulletin board in a common club room. On August 23, 1993, Griton invited readers of the yabbs bulletin board to contact the "Scream!" bulletin board service of which he was the "sysop" (systems operator) at a telephone number in Buenos Aires, Argentina. In pertinent part, at 00:10:34 on that day he posted:

> Call to:
>
> Scream! BBS
> +54.[0]1.72.6305
> 24-8 east time.

h/p, Pc Music, Cracks, VGA Stuff, friends...

To C001 Axes:
Name: INTER
pw: NET
Your sysop...

El Griton

Based on my training and experience, the first paragraph of this posting lists the time and telephone number at which the Scream! bulletin board service ("BBS") can be reached. The second paragraph gives a brief description of the types of information exchanged on the board. "H/p" is an abbreviation for "hacking" and "phreaking;" "cracks," a reference to "cracking." "Hacking" and "cracking" are slang terms for identifying and using systems' vulnerabilities to crack the security of computer systems and obtain unauthorized access to them. "Phreaking" refers to "phone phreaking," which is the practice of breaking into and misusing telephone systems. Phone phreaking includes obtaining unauthorized access to telephone exchanges which can be used to access computer networks and make long distance telephone calls without charge.[19]

[19] On February 22, 1996, FBI Special Agent James Hegarty and I contacted Carlos E. Maldonado, who is the Business Electronic Security Coordinator based in the United States for E.I. DuPont de Nemours and Company, Wilmington, Delaware with responsibility for coordinating electronic information security for DuPont in countries including Argentina. Maldonado confirmed he had contacted Harvard University regarding phone calls made from a DuPont Company telephone PBX (a private telephone switching system) into the FAS Harvard modem pool. DuPont has been conducting an internal investigation of the compromise and misuse of a PBX which services a DuPont Company plant in Mercedes, Argentina. Maldonado related that Jarvas V. Torres, a DuPont Company Manager located in Brazil responsible for Argentina, has reviewed telephone records for their PBX in Argentina and has determined that an unknown intruder obtained access to their PBX from outside the company and had made

The final paragraph gives an account name ("name") and password ("pw") through which a reader of the bulletin board posting on yabbs can access the Scream! bulletin board service.

73. In subsequent postings on the yabbs bulletin board in November, 1993, griton[20] sought information on how to "hack" into (break into) a particular kind of computer system, and described himself as a computer science student in his first year of study, and, in an aside, stated what a nice city he thought Chicago was.

74. The Federal Police of Argentina have determined that telephone number 72 6305, the number given by "griton" for his Scream! bulletin board, was in service in August, 1993, at the residence of Julio Rafael Ardita, his wife, their 21 year old son, Julio Cesar Ardita, and three minor children.[21] The Federal Police also have confirmed that Julio Cesar Ardita was more recently a student in applied sciences, a discipline which includes the computer sciences.

75. Julio Cesar Ardita and Julio Rafael Ardita both applied for United States visas in January, 1995. On that occasion, Julio Rafael Ardita listed his date of birth as July 9, 1946 and his

---

numerous telephone calls from Argentina to the FAS Harvard modem pool number at (617) 495-0635, to a residence in Chicago, Illinois and to other telephone exchanges in at least April and May, 1995.

[20] Ardita referred to himself both as "griton" and "El Griton." The return address line on the bulletin board postings read "griton@yabbs;" when the postings were signed, they were signed "El Griton."

[21] The oldest of these minor children, now 16, would have been approximately 14 at the time of the yabbs bulletin board postings.

occupation as retired military, consultant to Argentine Congress. On the same occasion, Julio Cesar Ardita listed his date of birth as March 28, 1974 and his occupation as student. Records of the Immigration and Naturalization Service indicate that only Julio Cesar Ardita travelled to the United States at that time and he listed his U.S. address during his stay as Chicago, Illinois.

76. Telecom Argentina has confirmed that someone broke into their computer network and from there accessed the FAS Harvard host during late 1995. While on the Telecom Argentina network, the Intruder installed files including the identifying "InfamousAngel" and "HotterThanMohaveInMyHeart," among others.

77. Telecom Argentina has determined that the intrusions into their host computer originated in Buenos Aires from a telephone number located in the apartment residence of Julio Cesar Ardita and his family. The telephone line from which the intrusions originated - 832 6305 - is the same as that on which the Scream!

bulletin board service had been operated earlier - 72 6305. The exchange was changed to 832 from 72 after August, 1993, during a restructuring of telephone service in Argentina.

Peter Garza
Special Agent
Naval Criminal Investigative Service

Subscribed and sworn before me this
_____ day of March, 1996.

MARIANNE B. BOWLER
UNITED STATES MAGISTRATE JUDGE

GLOSSARY

Computer Bulletin Board

A computer service which, among other things, allows users to post messages accessible to all other users of the service, just as an individual might tack a note to a cork bulletin board in a common club room.

Data Stream

An electronic communication within or between computers, e.g., in this case, one direction or the other between the FAS Harvard host and FAS Harvard router.

Hacker

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

Host computer

A computer connected to a network of computers, which maintains established user accounts for access to the network.

Internet

A global network of computer networks which allows for electronic communications between host computers belonging to different networks.

Keystroking

A means of monitoring the electronic communications so as to reconstruct and document the actual keystrokes which were typed at the user's computer terminal to transmit the electronic communications.

Modem

A piece of electronic equipment which converts the digital signal from a computer to an analog signal which can be transmitted across standard telephone lines. Modems are devices which make it possible to use a telephone to gain access to a computer system from the caller's personal computer.

Operating system

A computer's main program which controls the computer's resources and interprets commands by any other programs on the system.

Packet

A unit of information used to transmit electronic communications across networks. Information to be communicated across networks is broken down into small units, each of which is called a packet. Each 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 which identifies the host computer from which the message or data file was sent.

Pinga

A program used by the Intruder to obtain "root," or unlimited, access on a compromised network host.

Root access

Complete control over a UNIX computer system, through an account called "root," which allows access to all user accounts and all programs and files on the system. With "root" access, the user is able to view, alter and install files anywhere on the network host. Normally only the system administrator possesses root access.

Router

A device on a computer network which directs communications between different network segments.

Sniffer program

A program which intercepts electronic communications over the system on which it is placed. Specifically, it intercepts account/password combinations as the legitimate user transmits these combinations over the system in the form of commands. The program used by the Intruder ("sni256") stores the intercepted account/password combinations in a separate file ("test") for recovery later.