

UNITED STATES DISTRICT COURT
FOR THE [] DISTRICT OF []

)
IN RE APPLICATION OF THE)
UNITED STATES OF AMERICA FOR)
AN ORDER PURSUANT TO)
18 U.S.C. § 2703(d))
_____)

Mag. No.

Filed Under Seal

APPLICATION OF THE UNITED STATES
FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)

The United States of America, through its undersigned counsel, respectfully files under seal this ex parte application for an order pursuant to 18 U.S.C. § 2703(d) to require Attacker Host ("AHost"), an electronic communications service provider owned by [], located at [address] in the [] District of [], to provide records and other information pertaining to certain of its subscribers. The records and other information requested are set forth as Attachment A to the Application and to the proposed Order. In support of this Application, the United States says:

LEGAL AND FACTUAL BACKGROUND

1. The Office of [] of the United States [] and the U.S. Secret Service are investigating an attack on a [U.S. Government] computer, located at [], that occurred on [date]. The attack on the government computer is being investigated as a possible violation of, inter alia, 18 U.S.C. § 1030 (fraud and related activities in connection with computers).

2. Investigation to date of this incident provides reasonable grounds to believe that AHost has records and other information pertaining to certain of its subscribers that are relevant and material to an ongoing criminal investigation. Because AHost is an electronic communications service provider -- that is, it provides its subscribers access to electronic communication services, including e-mail and the Internet -- 18 U.S.C. § 2703 sets out particular requirements that the government must meet in order to obtain access to the records and other information it is seeking.

3. Here, the government seeks to obtain basic subscriber information, as well as records and other information pertaining to certain subscribers of AHost. To obtain basic subscriber information, the government needs only a subpoena. 18 U.S.C. § 2703(c)(1)(C). To obtain records and other information pertaining to subscribers of an electronic communications service, the government must comply with the dictates of section 2703(c)(1)(B), which provides, in pertinent part:

A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to a governmental entity only when the governmental entity --

....

(ii) obtains a court order for such disclosure under subsection (d) of this section;

....

4. Section 2703(d), in turn, provides (in pertinent part):

(d) Requirements for court order.--A court order for disclosure under subsection . . . (c) may be issued by any court that is a court of competent jurisdiction described in section 3127(2)(A)¹ and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the . . . records or other information sought, are relevant and material to an ongoing criminal investigation. . . . A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

¹ "Court of competent jurisdiction" includes a district court of the United States as well as a United States Magistrate. 18 U.S.C. § 3127(2)(A).

Accordingly, this application sets forth the facts showing that there are reasonable grounds to believe that the records and other information sought from AHost are relevant and material to the ongoing criminal investigation of the attack on the government computer.

THE RELEVANT FACTS

[THIS SECTION SETS FORTH THE "SPECIFIC AND ARTICULABLE FACTS" REQUIRED BY § 2703(d) IN SUPPORT OF THE APPLICATION]

5. The government computer was attacked and altered by an unauthorized person on [date]. On [date], Special Agent Cybercop began an authorized monitoring of all computer traffic destined for the computer that hosts the government computer. (That computer is identified as "000.0.00.00.")

6. On [date], at approximately [time], SA Cybercop noticed unusual activity on the government computer. Specifically, a person was signed on to the computer using the identifier of "LP," which is ordinarily reserved for the printer ("Line Printer"). SA Cybercop immediately removed the government computer from the network in order to avoid exposing the government computer to further attack.

7. The evidence shows that the user was a sophisticated computer operator who demonstrated an interest in controlling the computer's operations and who probably had utilized this computer previously. The person using the "LP" account, upon signing in, immediately accessed a "hidden" directory (set of files) which contained two important files. One of those files was a copy of a "password" file, dated []. Even though the passwords in the password file are encrypted because of their obvious importance, a sophisticated computer operator can often,

given enough time, break the encryption scheme and obtain access to accounts with unlimited privileges, known as the "superuser" account.

8. In fact, the other file stored in the hidden directory was a program that, if executed, would provide the account with superuser privileges. The intruder executed this program and thus acquired the power to access or alter anything on the system.

9. The intruder immediately took advantage of these additional privileges by copying important system operation files and network operation files. The intruder also took advantage of the increased status by running programs designed to ascertain which other accounts on the government computer were being utilized and what programs were running on the government computer. It was at this point that SA Cybercop disconnected the government computer from the network.

10. Evidence of the attack on the government computer includes the Internet Protocol address of the remote computer used by the attacker. An Internet Protocol ("IP") address is a unique numeric identifier assigned to every computer attached to the Internet. An Internet service provider (ISP) such as AHost normally controls a range of several hundred (or even thousands of) IP addresses, which it assigns to its customers for their use.

11. IP numbers for individual user accounts (such as are sold by ISPs to the general public) are usually assigned "dynamically": each time the user dials into the ISP to connect to the Internet, the customer's machine is randomly assigned one of the available IP addresses controlled by the ISP. The customer's computer retains that IP address for the duration of that session (i.e., until the user disconnects), and the IP address cannot be assigned to another user during that

period. Once the user disconnects, however, that IP address becomes available to other customers who dial in thereafter. Thus, an individual customer's IP address normally differs each time he dials into the ISP. By contrast, an ISP's business customer will commonly have a permanent, 24-hour Internet connection to which a "static" (i.e., fixed) IP address is assigned.

12. A review of the government's computer audit logs revealed that the person using the "LP" account on [date] had accessed the computer from IP address 999.999.999.999. Prior to [date of attack], the router logs, which track only unsuccessful attempts to connect to the government computer, reveal at least two attempts from IP address 999.999.999.998. Those attempts, on [date prior to attack], included an active probe of the government computer and an attempt, using a network communications program called "telnet," to connect to the government computer. Public network information reveals that IP addresses 999.999.999.999 and 999.999.999.998 are associated with AHost. The number of successful connections from AHost to the government computer is not known.

13. Internet records reveal that AHost is registered to [name of person or company]. Those records list a telephone number of [] and a mailing address of [].

14. The records we are requesting (attached as Attachment A to this Application and Order) are in four parts. Part A consists of AHost's "User Connection Logs" from [date of first probe] through the date of the Court's Order, for all connections to the Government computer (000.0.00.00) from AHost. The information on those logs should include the date and time of connection and disconnection, the method of connection, the data transfer volume, the subscriber account associated with the connection, and information regarding the session, including connect

and disconnect times, other session information, and other systems to which the AHost user connected during that session.

15. Part B consists of information that will help the investigation identify the individual or individuals who effected the connections described in Part A by providing the subscriber's name, address, telephone number, e-mail address, credit card information, other identifying information (such as date of birth, social security number, billing information, and driver's license number), and any other record or information pertaining to the account.

16. Parts C and D consists of information that will help the investigation identify the individual or individuals who effected the [date] probe and telnet attempts and the [later date] unauthorized access, in the event that the user connection logs called for by Parts A and B are inadequate or incomplete. In Part C, for any subscriber assigned the IP address 999.999.999.999 or 999.999.999.998 on the relevant dates, we ask for the subscriber's name, address, telephone number, e-mail address, credit card information, and other identifying information (such as date of birth, social security number, billing information, and driver's license number). (If the information is not available by IP number, the order directs AHost to identify anyone logging onto the service on the identified dates.)

17. Part D consists of AHost's "User Connection Logs" from [date] through the date of the Court's Order, for each subscriber identified in Part C. The information on those logs should include the date and time of connection and disconnection, the method of connection to AHost, the volume of data transfer, and information related to successive connections to other systems.

18. The information requested should be readily accessible to AHost by computer search, and its production should not prove to be burdensome.

19. The United States further requests, pursuant to 18 U.S.C. § 2705(b), that this Application and Order be sealed by the court until such time as the court directs otherwise, and that AHost be ordered not to disclose the existence or content of the Order, except to the extent necessary to carry out the Order. Disclosure of the Order at this time to AHost's subscribers or to the public at large would seriously jeopardize the investigation.

WHEREFORE, the United States respectfully requests that the Court enter the attached Order directing AHost to provide the United States with the records and information described in Attachment A to the Order, further ordering that the Application and Order be sealed, and further ordering that AHost be directed not to disclose the existence or content of the Order, except to the extent necessary to carry out the Order.

[IF "AHOST" IS AN EDUCATIONAL INSTITUTION RATHER THAN A COMMERCIAL PROVIDER, INCLUDE THE FOLLOWING ADDITIONAL LANGUAGE:

In addition, the United States notes that [institution] is an educational institution potentially governed by the Baker Act, 20 U.S.C. § 1232g, which generally bars educational institutions receiving federal funds from disclosing student records to third parties absent parental consent. The United States respectfully requests that [institution]'s compliance with the non-disclosure provision of the Order be deemed authorized under 20 U.S.C. § 1232g(b)(1)(J)(ii).]

Respectfully submitted,

Assistant United States Attorney
_____ District of _____

UNITED STATES DISTRICT COURT
FOR THE [] DISTRICT OF []

IN RE APPLICATION OF THE)	Mag. No.
UNITED STATES OF AMERICA FOR)	
AN ORDER PURSUANT TO)	
18 U.S.C. § 2703(d))	Filed Under Seal

ORDER

This matter having come before the court pursuant to an application under Title 18, United States Code, Section 2703(c), which application requests the issuance of an order under Title 18, United States Code, Section 2703(d) directing AHost, an electronic communications service provider owned by [name of person or company, located at [address] in the [] District of [], to disclose certain records and other information, as set forth in Attachment A to the Application, the court finds that the applicant has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation.

IT APPEARING that the information sought is relevant and material to an ongoing criminal investigation, and that disclosure to any person of this investigation or this application and order entered in connection therewith would seriously jeopardize the investigation;

IT IS ORDERED pursuant to Title 18, United States Code, Section 2703(d) that AHost will, within three days of the date of this Order, turn over to agents of the U.S. Secret Service or to agents of the [] the records and other information as set forth in Attachment A to this Order.

IT IS FURTHER ORDERED that the application and this Order are sealed until otherwise ordered by the court, and that AHost shall not disclose the existence of this application and/or Order of the court, or the existence of the investigation, to the listed subscriber or to any other person (except as necessary to carry out this Order) unless and until authorized to do so by the Court. **[IF THE PROVIDER IS AN EDUCATIONAL INSTITUTION, INCLUDE THE FOLLOWING: [institution]'s compliance with the non-disclosure provision of this Order shall be deemed authorized under 20 U.S.C. § 1232g(b)(1)(J)(ii).]**

DATED: _____

UNITED STATES MAGISTRATE

ATTACHMENT A

You are to provide the following information:

- A. User Connection Logs for all connections from AHost to the government computer 000.0.00.00 for the time period beginning [date] through and including [date] to include, for each connection:
1. Connection time and date to 000.00.00.0;
 2. Disconnect time and date from 000.00.00.0;
 3. Method of connection (e.g., telnet, ftp, http);
 4. Data transfer volume (e.g., bytes);
 5. The subscriber account associated with the connection.
 6. Any information related to the session during which the connection to AHost was open, including:
 - a. Connection time and date to AHost;
 - b. Disconnect time and date from AHost;
 - c. Method of connection to AHost (e.g., SLIP, PPP, shell dial-up, telnet, ftp, http);
 - d. Ancillary and source information relating to the connection to AHost, such as the IP address of the source of the connection or connection speed;
 - e. Connection information for other systems to which user connected via AHost during that session, including:
 - i. Connection destination;
 - ii. Connection time and date;
 - iii. Disconnect time and date;
 - iv. Method of connection to system (e.g., telnet, ftp, http);

- v. Data transfer volume (e.g., bytes);
 - vi. Any other record or information pertaining to the connection from AHost.
 - f. Any other record or information pertaining to the connection to AHost.
- B. Subscriber information for each subscriber account identified in Part A, above. For each such subscriber, the information shall include:
 - 1. The subscriber's name;
 - 2. The subscriber's address;
 - 3. The subscriber's telephone number;
 - 4. The subscriber's e-mail address;
 - 5. Any other information pertaining to the identity of the subscriber, including, but not limited to, date of birth, social security number, driver's license number, billing information (including type and number of credit cards or bank accounts).
 - 6. Any other record or information pertaining to the subscriber account, including length of account activation, type of service, special requested services, records of contacts between the subscriber and AHost, or other service notes.
- C. All subscriber information for each subscriber who, for any session that began or ended on [Dates] was assigned the IP address 999.999.999.999 or 999.999.999.998; or, if that information is unavailable, all subscriber information for each subscriber who connected to AHost on [dates]. For each such subscriber, the information shall include:
 - 1. The subscriber's name;
 - 2. The subscriber's address;
 - 3. The subscriber's telephone number;
 - 4. The subscriber's e-mail address;
 - 5. Any other information pertaining to the identity of the subscriber, including, but not limited to, date of birth, social security number, driver's license number, billing information (including type and number of credit cards or bank accounts).

6. Any other record or information pertaining to the subscriber account, including length of account activation, type of service, special requested services, records of contacts between the subscriber and AHost, or other service notes.
- D. User connection logs for all users identified in Part C, above, for the time period beginning [date] through and including [date] to include, for each connection to AHost,
1. Connection time and date to AHost;
 2. Disconnect time and date from AHost;
 3. Method of connection to AHost (e.g., SLIP, PPP, shell dial-up, telnet, ftp, http);
 4. Data transfer volume (e.g., bytes);
 5. Ancillary information relating to the connection to AHost, such as the IP address of the source of the connection or connection speed;
 6. Any other record or information pertaining to the connection to AHost.
 7. Connection information for other systems to which user connected via AHost, including:
 - a. Connection destination;
 - b. Connection time and date;
 - c. Disconnect time and date;
 - d. Method of connection to system (e.g., telnet, ftp, http);
 - e. Data transfer volume (e.g., bytes).

The information should be provided both on 8.5x11-inch paper printouts or photocopies and, where maintained in electronic form, on 3.5-inch IBM-formatted floppy disks.