

JK

JUN 12 2007

**MICHAEL W. DOBBINS
CLERK, U.S. DISTRICT COURT**

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

JUDGE CASTILLO

No. **07 CR 379**

MAGISTRATE JUDGE VALDEZ

Violations: Title 18, United States Code,
Section 1030(a)(5)(A)(i), (B)(i), & (B)(ii)

UNITED STATES OF AMERICA)
)
)
 v.)
)
 JAMES C. BREWER)

COUNT ONE

The SPECIAL AUGUST 2006-1 GRAND JURY charges:

1. At times material to the indictment:

a. The Cook County Bureau of Health Services ("CCBHS") was a division of the Cook County government that administered and operated health care centers throughout the City of Chicago and surrounding suburbs, including the Ambulatory and Community Health Network of Cook County, Cermak Health Services of Cook County, John H. Stroger, Jr. Hospital of Cook County, Oak Forest Hospital of Cook County, and Provident Hospital of Cook County. Computers located at facilities operated by the CCBHS were connected to one another as part of a computer network.

b. Personnel at CCBHS facilities, including medical personnel, relied upon computers to perform various functions, such as managing and accessing patient care records and filling prescriptions for inpatient hospital residents. Personnel at CCBHS facilities relied directly upon computers in the provision of medical services and testing, such as fetal monitoring, the operation of scanning and imaging equipment, and laboratory testing.

c. Defendant JAMES C. BREWER was a resident of Arlington, Texas.

d. A "bot" was a computer program that could be implanted on a computer without authorization to perform various functions at the direction of the person who controlled the "bot." The controller of the "bot" accomplished the installation of the "bot" by using a computer or computers to electronically scan or search local networks or the Internet for computers with particular vulnerabilities or security weaknesses, such as the absence of a firewall, and using computer code written to take advantage of those vulnerabilities or weaknesses to compromise or "hack" into the computer. Once the computer was compromised, the "bot" code was installed on the computer and caused the computer to perform certain functions at the direction of the person controlling the bot, such as allowing the controller of the "bot" to access the computer.

e. A "botnet" was a network of computers infected with "bots." The "bots" were configured to automatically establish Internet connections with Internet Relay Chat ("IRC") servers and to receive commands in the form of topics posted in specific "chat-rooms" or "channels" on the IRC servers. The "botnet" controller was then able to control the "botnet" by connecting to the appropriate "chat-room" or "channel" on the IRC servers and issuing commands to the bots in the form of topics. An illicit market existed for the purchase and sale of "botnets."

f. One command commonly issued to a computer infected with a "bot" was for the computer to scan local networks or the Internet for other computers to infect with

the "bot," thereby increasing the size and power of the "botnet." The process of scanning for vulnerable computers to add to the "botnet" could generate a large amount of network traffic, particularly within local networks. The increase in network traffic could be sufficient to interrupt and disable normal network communications and functions, thereby rendering network computers unable to perform their intended functions, and requiring significant repairs in order to resume those normal functions.

2. Prior to in or about October 2006, defendant JAMES C. BREWER obtained and designed malicious software or "bots" to infect computers belonging to others without the knowledge or authorization of the owners of the computers for the purpose of establishing a network of infected computers or "botnet."

3. Defendant JAMES C. BREWER programmed the malicious software or "bots" to cause the infected computers to establish Internet connections to IRC channels located on computer servers associated with, among others, the Internet domain names "http.an1malming.com" and "http.fire-servers.net." Defendant controlled the IRC "chat-rooms" or "channels" located on these computer servers and used them to issue commands to the infected computers that connected to the IRC "channels."

4. The commands issued to infected computers included commands to continuously scan local networks and the Internet for other computers that were vulnerable to infection and, upon the identification of such computers, to infect the computers with the malicious software or "bots" designed and controlled by defendant.

5. The malicious software or "bots" designed and controlled by defendant JAMES C. BREWER infected over 10,000 computers across the world, including computers located at CCBHS facilities such as the Nuclear Medicine Department and Oncology-Radiation Therapy Department at John H. Stroger Hospital, and computers in the Pharmacy Department at Oak Forest Hospital. The "bots" caused the infected computers to, among other things, repeatedly freeze or reboot without notice, thereby causing significant delays in the provision of medical services and access to data by CCBHS personnel. The computers at CCBHS' facilities continued to experience problems resulting from the "bots" through in or about December 2006, and in excess of 1,000 hours were spent by CCBHS personnel and private vendors attempting to remedy the problems.

6. In or about October 2006, at Chicago, in the Northern District of Illinois, and elsewhere,

JAMES C. BREWER,

defendant herein, knowingly caused the transmission of a program, information, code, and command, namely, malicious "bot" source code, and as a result of that conduct intentionally caused damage, without authorization, to computers used in interstate commerce and communication, namely, computers belonging to CCBHS, which conduct caused the modification and impairment, and potential modification and impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals;

In violation to Title 18, United States Code, Section 1030(a)(5)(A)(i), (B)(ii).

COUNT TWO

The SPECIAL AUGUST 2006-1 Grand Jury further charges:

1. The allegations of paragraphs 1 through 5 of Count One of this indictment are realleged and incorporated as though fully set forth here.

2. In or about October 2006, at Chicago, in the Northern District of Illinois, and elsewhere,

JAMES C. BREWER,

defendant herein, knowingly caused the transmission of a program, information, code, and command, namely, malicious "botnet" source code, and as a result of that conduct intentionally caused damage, without authorization, to computers used in interstate commerce and communication, namely, computers belonging to CCBHS, which conduct caused an aggregate loss of at least \$5,000 to CCBHS during a one-year period;

In violation to Title 18, United States Code, Section 1030(a)(5)(A)(i), (B)(i).

A TRUE BILL:

FOREPERSON

UNITED STATES ATTORNEY