UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

December 2007 Grand Jury

UNITED STATES OF AMERICA, Plaintiff, v. LEE GRAHAM WALKER, aka "SorCe," aka "Fight," aka "Ago-abig," and AXEL GEMBE, aka "Ago," Defendants.	Case No. CR CR 08- CR08-01168 I N D I C T M E N T [18 U.S.C. § 371: Conspiracy; 18 U.S.C. § 1030(a)(5)(A)(i), (a)(5)(B)(i), (c)(4)(A): Transmission of a Code, Information, Program, or Command to a Protected Computer]

The Grand Jury charges:

INTRODUCTORY ALLEGATIONS

At all times relevant to this Indictment:

ASHLEY

1. Paul Garrett Ashley ("Ashley") was the founder, owner, and computer systems administrator of Creative Internet Techniques ("CIT"), an Internet Service Provider based in Powell, Ohio. CIT ran a network known as "Foonet" that provided web hosting and other computer services to customers.

EMS/MCK

ECHOUAFNI

2. Jay R. Echouafni ("Echouafni"), also known as ("aka") Saad Echouafni, was the owner and Chief Executive Officer of Orbit Communication Corporation ("Orbit"), a Massachusetts corporation based in Sudbury, Massachusetts. Orbit provided home satellite systems to customers through its website, www.orbitsat.com, and its sales department.

WEAKNEES

3. Weaknees was an online business based in Los Angeles, California, that sold and upgraded personal digital video recorders ("DVRs"), including "TIVO" and other DVRs. Weaknees sold its products through its website on the Internet, www.weaknees.com. Weaknees had a strategic alliance with WebClick Concepts/Rapid Satellite. Weaknees had discussed having a strategic alliance with Orbit and Echoufani, but the alliance did not take place.

RAPID SATELLITE

4. Rapid Satellite was an online business owned by WebClick Concepts, Inc., in Miami, Florida. Rapid Satellite sold home satellite television systems to customers through its website, www.rapidsatellite.com, and sales department. Rapid Satellite was a competitor of Orbit.

AXEL GEMBE

5. Defendant AXEL GEMBE ("defendant GEMBE"), aka "Ago," resided in Germany, and designed and updated software used to create a robot network of computers called "agobot," which he provided for use by himself and defendant LEE GRAHAM WALKER.

LEE GRAHAM WALKER

6. Defendant LEE GRAHAM WALKER ("defendant WALKER"), aka "SorCe," aka "Fight," and aka "Ago-abig," resided in the United Kingdom and used a robot network of computers, "agobot," with defendant GEMBE.

COMPUTER TERMINOLOGY

7. Internet Protocol ("IP") Address: A unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses, which they assign to their subscribers. No two computers on the Internet can have the same IP address at the same time. Thus, at any given moment, an IP address is unique to the computer to which it has been assigned.

8. Domain: A domain is a group of Internet devices (such as computers, including hand-held personal data assistants) that are owned or operated by a specific individual, group, or organization. Devices within a domain have IP addresses within a certain range of numbers, and are usually administered together.

9. Domain name: A domain name identifies a computer or group of computers on the Internet belonging to a particular domain (that is, to an individual or group of individuals), and corresponds to one or more IP addresses within a particular range. Domain names are typically strings of alphanumeric characters, with each "level"

of the domain delimited by a period. For example, www.microsoft.com is a domain name belonging to the Microsoft Corporation, but is also a part of the ".com" domain. A domain name can provide information about the organization, ISP, and physical location of a particular user of the Internet.

10. Bot: The term "bot" is derived from the word "robot" and commonly refers to a software program that performs repetitive functions, such as indexing information on the Internet. Bots have been created to perform tasks automatically on IRC servers. Bot also refers to computers that have been infected with a program used to control or launch DDOS attacks (as defined in paragraph 12 below) against other computers.

11. Botnet: A "botnet" is typically a network of computers infected with bots that are used to control or attack computer systems. Botnets often are created by spreading a computer virus or worm that propagates throughout the Internet, gains unauthorized access to computers on the Internet and infects the system with a particular bot program. The botnet is then controlled by a user, often through the use of a specified IRC channel. A botnet can consist of tens of thousands of infected computers. The unsuspecting infected or compromised computers are often referred to as "zombies" or "drones" and are used in DDOS attacks.

12. DDOS Attack: A distributed denial of service ("DDOS") attack is a type of malicious computer activity in which an attacker causes a network of compromised computers to "flood" a victim computer with large amounts of data or specified computer commands. A DDOS attack typically renders the victim computer unable to handle legitimate network traffic and often the victim

computer will be unable to perform its intended function and legitimate users are denied the services of the computer. Depending on the type and intensity of the DDOS attack, the victim computer and its network may become completely disabled and require significant repair.

13. SynFlood: A "SynFlood" is a type of DDOS attack in which a computer or network of computers send a large number of "Syn" data packets to a targeted computer. Syn packets are sent by a computer that is requesting a connection with a destination computer. A SynFlood typically involves thousands of compromised computers in a botnet that flood a computer system on the Internet with "Syn" packets containing false source information. The flood of Syn packets cause the victimized computer to use all of its resources to respond to the requests and render it unable to handle legitimate traffic.

14. Hypertext Transfer Protocol ("HTTP"): An Internet protocol for the transfer of information that defines the way Web browsers and Web servers communicate with each other. For example, when a computer user enters a domain name or IP address into their web browser, the computer user is actually sending an HTTP command to the Web server directing it to fetch and transmit the requested web page.

15. HTTPFlood: An "HttpFlood" is a type of DDOS attack in which a computer or network of computers send a large number of HTTP requests to a targeted web server, overwhelming the targeted web sever's ability to respond.

16. IRC: Internet Relay Chat ("IRC") is a network of computers connected through the Internet that allows users to

communicate (or chat) with others in real time. IRC users utilize specialized client software to use the service and can access a "channel" that is administered by one or more "operators" or "ops." IRC channels sometimes are dedicated to a topic and are identified by a pound sign and a description of the topic such as "#miamidolphins." IRC channels also are used to control botnets that are used to launch DDOS attacks.

17. Spoofing: A technique used by attackers wherein a fake IP address is used so that the recipient of an IP packet does not receive the IP address of the actual sender.

///

///

COUNT ONE

[18 U.S.C. § 371]

OBJECT OF THE CONSPIRACY

18. The Grand Jury hereby repeats and re-alleges paragraphs 1 through 17 of this Indictment.

19. Beginning on an unknown date, and continuing through on or about November 14, 2003, in Los Angeles County, within the Central District of California, and elsewhere, defendant WALKER, defendant GEMBE, co-conspirator Echouafni, co-conspirator Ashley, and others known and unknown to the grand jury, conspired and agreed with each other to knowingly transmit a program, information, code, and command, and as a result of such conduct, intentionally cause damage without authorization to a protected computer, in violation of 18 U.S.C. § 1030(a)(5)(A)(i), (a)(5)(B)(i), (c)(4)(A).

MEANS BY WHICH THE OBJECT OF THE CONSPIRACY WAS TO BE ACCOMPLISHED

20. The object of the conspiracy was to be accomplished as follows:

a. Defendant GEMBE would create a botnet, which he would maintain with defendant WALKER.

b. Co-conspirator Echouafni would contact co-conspirator Ashley and order him to launch an attack against the websites www.weaknees.com and www.rapidsatellite.com to make them inaccessible on the Internet.

c. Co-conspirator Ashley would contact defendant WALKER and other co-conspirators and coordinate the DDOS attacks against the particular websites.

d. The co-conspirators, including defendant WALKER, would cause botnets that they controlled, or to which they had access, to launch DDOS attacks against the websites, rendering them inaccessible to legitimate users on the Internet.

OVERT ACTS

21. In furtherance of the conspiracy, and to accomplish the object of the conspiracy, defendant WALKER, defendant GEMBE, co-conspirator Echouafni, co-conspirator Ashley, and others known and unknown to the grand jury, committed various overt acts within the Central District of California and elsewhere, including the following:

a. On or about August 19, 2003, defendant GEMBE had an IRC chat with defendant WALKER in which he informed defendant WALKER that he was testing "agobot3," software that he had designed to create and maintain a botnet.

b. On or about August 19, 2003, defendant GEMBE informed defendant WALKER that they needed a domain name for the botnet.

c. On or about August 19, 2003, defendant WALKER created and registered the domain name "bunghole.myslqd.com."

d. On or about August 19, 2003, defendant WALKER asked defendant GEMBE via IRC whether he had added "the synflood in from the old bot yet" to agobot3.

e. On or about August 19, 2003, defendant GEMBE stated via IRC that he had not added synflood, although he was "at it."

f. On or about August 20, 2003, defendants GEMBE and WALKER discussed the botnet via IRC and, during the conversation, GEMBE stated that he was implementing the "synflood."

g. Shortly thereafter, on or about August 20, 2003, defendant GEMBE informed defendant WALKER via IRC that he "got the synflood built in" and "I have new bots with much more commands and syn flood added."

h. On or about August 20, 2003, defendants WALKER and GEMBE discussed via IRC testing the botnet to conduct a DDOS attack.

i. On or about August 20, 2003, via IRC, defendant WALKER told defendant GEMBE that he had "some big shit to hit for a long time :)" and he wanted "50k bots hitting . . . an IP for 20 sec[onds]."

j. On or about August 20, 2003, defendant GEMBE informed defendant WALKER via IRC that "synflood works."

k. On or about August 20, 2003, defendants WALKER and GEMBE tested a DDOS attack, with WALKER reporting via IRC that "im not even getting anything" "it's not like ur old flood not as good."

l. On or about August 20, 2003, in response to problems with the DDOS attack test, defendant GEMBE informed defendant WALKER via IRC that he was "debugging it."

m. On or about August 21, 2003, defendant WALKER contacted defendant GEMBE via IRC to ask "hows the syn coming."

n. On or about August 21, 2003, defendant GEMBE informed defendant WALKER via IRC that "synflood works, i tested [the synflood] on some sites yesterday." Defendant GEMBE noted that he "knocked myself offline yesterday while testing."

o. On or about August 21, 2003, during a DDOS test, defendant WALKER complained via IRC to defendant GEMBE that "it

doesn't spoof this isn't like the old attack it's not a very good flood i need it to spoof. . . they will be traced easy man."

p. On or about August 21, 2003, defendant GEMBE responded via IRC that he would "do completely random." Defendant GEMBE informed defendant WALKER that he would "probably implement" other types of DDOS attacks and he "could also do a http flood."

q. On or about August 21, 2003, defendant WALKER noted via IRC that "a dns flood would be good too," although he "just mainly i need that spoofed syn."

r. On or about August 24, 2003, during an IRC discussion, defendant WALKER asked defendant GEMBE, "did u sort that syn thing out."

s. On or about August 24, 2003, defendant GEMBE told defendant WALKER via IRC that he had worked out the syn issues, that it "spoofs now," and that he "brought hosts down with it today all after [a] few seconds."

t. On or about August 24, 2003, defendants WALKER and GEMBE discussed via IRC a test that they were doing, with defendant WALKER noting that there was "no spoof at all all real ip's. . . . thats not a good flood someone can track it in seconds."

u. On or about August 24, 2003, defendant WALKER told defendant GEMBE via IRC to "get 50K bots and fix that syn and stuff ;)."

v. On or about August 25, 2003, defendant WALKER told defendant GEMBE via IRC that "all you need to do now is make it spoof" because it "doesn't spoof man."

w. On or about September 4, 2003, defendant WALKER asked defendant GEMBE via IRC chat "did u ever make the udp or icmp

flood."

x. On or about September 4, 2003, defendant GEMBE responded that he had not done so yet, but that "i will addd the rest of the ddoses today probably."

y. On or about September 4, 2003, defendant WALKER told defendant GEMBE via IRC that "i need like 10,000 bots with that syn flood thats already on maybe and a upd flooder and icmp then I will be happy."

z. On or about September 4, 2003, via IRC, defendant GEMBE advised defendant WALKER that he was going to add an additional attack option (pan-attack) in agobot3, and provided defendant WALKER with a link to the code he was going to use. Defendant GEMBE also mentioned an article on DDOS attacks.

aa. On or about September 4, 2003, defendant WALKER responded via IRC that "pan is old and it's easy filterable."

bb. On or about September 4, 2003, via IRC, defendant GEMBE agreed that it was filterable, but that it "must be hard for joe-average to filter."

cc. On or about September 4, 2003, defendant WALKER responded via IRC, "yea but the things i fuck aren't average they are people like akamai they are people like microsoft they are well filtered."

dd. On or about September 24, 2003, defendant GEMBE told defendant WALKER via IRC that "ive started with my http flooder/visiter which will imitate users" but that "it will be in the next version cause im really busy atm."

ee. On or before October 6, 2003, co-conspirator Echouafni contacted co-conspirator Ashley and discussed launching

an attack against Weaknees and Rapid Satellite, both competitors of Echouafni's company, Orbit.

ff. On or about October 6, 2003, co-conspirator Ashley contacted defendant WALKER and other co-conspirators and instructed them to launch a DDOS attack against www.weaknees.com and www.rapidsatellite.com.

gg. On or about October 6, 2003, the co-conspirators, including defendant WALKER, launched a series of SynFlood DDOS attacks against www.weaknees.com and www.rapidsatellite.com.

hh. On or about October 6, 2003, co-conspirator Echouafni paid co-conspirator Ashley $1,000 through the PayPal online payment system.

ii. On or about October 9, 2003, the co-conspirators, including defendant WALKER, launched a series of SynFlood DDOS attacks against wwww.rapidsatellite.com.

jj. On or about October 10, 2003, defendant WALKER launched a series of SynFlood DDOS attacks against www.rapidsatellite.com and Rapid Satellite's webhosting company, Datapipe, that were severe enough to cause Datapipe to drop Rapid Satellite as a client.

kk. On or about October 10, 2003, co-conspirator Echouafni contacted Rapid Satellite's owner and offered to host Rapid Satellite's web site for $5,000 a month.

ll. On or about October 10, 2003, co-conspirators launched a series of DDOS attacks against www.weaknees.com that were severe enough to cause Weaknees' web hosting service, Lexiconn, to drop Weaknees as a client.

mm. On or about October 10, 2003, co-conspirator

Eschoufani paid co-conspirator Ashley another $1,000 through PayPal.

nn. After Weaknees was able to re-establish a public website with a new web hosting service, Rackspace, on or about October 11, 2003, on that same date, defendant WALKER attempted a SYN Flood DDOS attack against www.weaknees.com (IP address 69.20.6.120).

oo. On or about October 11, 2003, co-conspirator Ashley transferred $900 to defendant WALKER via PayPal.

pp. After Rapid Satellite was able to re-establish a public website with a new web hosting service, Akamai, on or about October 12, 2003, defendant WALKER launched a series of SynFlood DDOS attacks against www.rapidsatellite.com.

qq. On or about October 12, 2003, defendant WALKER conducted reconnaissance of www.weaknees.com using a unixcon.net account in the name of "DODOL," which he controlled.

rr. On or about October 12, 2003, defendant WALKER launched a series of SynFlood DDOS attacks against www.weaknees.com.

ss. On or about October 14, 2003, defendant WALKER launched a series of SynFlood DDOS attacks against www.weaknees.com and www.rapidsatellite.com.

tt. On or about October 14, 2003, defendant WALKER launched a series of HTTP Flood DDOS attacks against www.weaknees.com and www.rapidsatellite.com.

uu. On or about October 15, 2003, co-conspirator Ashley transferred $400 to defendant WALKER via Paypal.

vv. On or about October 15, 2003, defendant WALKER

conducted reconnaissance of www.weaknees.com using a unixcon.net account in the name of "DODOL," which he controlled.

ww. On or about October 20, 2003, co-conspirator Ashley transferred $675 to defendant WALKER via Paypal.

xx. On or about October 26, 2003, defendant GEMBE via IRC informed defendant WALKER that they had to update the bot because he had made "a bug" in the software, which he just discovered.

yy. On or about October 26, 2003, defendant WALKER informed defendant GEMBE that he needs "the bots for this proxy thing and spoofed http floods and stuff" and that they needed a "better spoofed flooder."

zz. On or about October 26, 2003, defendant GEMBE noted that "the http flood works very good." Defendant GEMBE then showed defendant WALKER via IRC the changes made to the http flood, how to launch an attack, and the effect of using the attack.

aaa. On or about October 26, 2003, defendant WALKER informed defendant GEMBE that "well fbi are watching some servers im hitting so it needs to be very spoofed the hits."

bbb. On or about October 26, 2003, co-conspirator Ashley transferred $675 to defendant WALKER via Paypal.

ccc. On or about October 26, 2006, defendant WALKER transferred $60 to defendant GEMBE via Paypal.

///

///

COUNT TWO

[18 U.S.C. §§ 1030(a)(5)(A)(i), (a)(5)(B)(i), (c)(4)(A)]

22. The Grand Jury hereby repeats and re-alleges paragraphs 1 through 17 and 21 of this Indictment.

23. Beginning on or about October 6, 2003, and continuing through on or about October 16, 2003, in Los Angeles County, within the Central District of California, and elsewhere, defendant WALKER and defendant GEMBE knowingly transmitted a program, information, code and command, and as a result of such conduct, intentionally caused damage without authorization, to a protected computer, namely, defendant WALKER and defendant GEMBE launched distributed denial of service attacks against the protected computers of www.weaknees.com, and as a result of such conduct, caused loss during a one-year period aggregating at least $5,000 in value.

A TRUE BILL

/S/

Foreperson

THOMAS P. O'BRIEN
United States Attorney

CHRISTINE C. EWELL
Assistant United States Attorney
Chief, Criminal Division

MARK C. KRAUSE
Assistant United States Attorney
Deputy Chief, Cyber and Intellectual Property Crimes Section

ERIK M. SILBER
Assistant United States Attorney
Cyber and Intellectual Property Crimes Section