UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

February 2005 Grand Jury

UNITED STATES OF AMERICA, Plaintiff, v. JEANSON JAMES ANCHETA, Defendant.	Case No. CR 05-1060 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), and 1030(b): Attempted Transmission of a Code, Information, Program or Command to a Protected Computer; 18 U.S.C. §§ 1030(a)(5)(A)(i) and (a)(5)(B)(v): Transmission of a Code, Information, Program or Command to a Protected Computer Used By a Government Entity; 18 U.S.C. § 1030(a)(4): Accessing Protected Computers to Conduct Fraud; 18 U.S.C. § 1956(a)(1)(A)(i): Promotional Money Laundering; 21 U.S.C. § 853: Criminal Forfeiture]

The Grand Jury charges:

INTRODUCTORY ALLEGATIONS

At all times relevant to this indictment:

DEFENDANT JEANSON JAMES ANCHETA

1. Defendant JEANSON JAMES ANCHETA ("ANCHETA") was an individual residing in Los Angeles County, within the Central District of California.

2. ANCHETA possessed at least one computer at his residence, and accessed the Internet from the telephone line located there.

3. ANCHETA used the following email accounts: gridin@gmail.com; iamjames85@yahoo.com, jazzsanjoy@peoplepc.com, resili3nt@gmail.com, resilient24@earthlink.net, resjames@sbcglobal.net, and resjames@yahoo.com.

4. ANCHETA used the following user name: ir Resilient.

5. ANCHETA used the following nicknames: aa, fortunecookie, gjrj, Resilient, ResilienT, ServiceMode, and SHK.

UNINDICTED CO-CONSPIRATOR IN BOCA RATON, FLORIDA

6. An unindicted co-conspirator residing in Boca Raton, Florida (hereinafter referred to as "SoBe"), was a computer user with experience in launching computer attacks, and as set forth below, was involved in the conspiracy to access protected computers to commit fraud.

7. SoBe possessed at least one computer at the Florida residence, and accessed the Internet from a cable line located there.

8. SoBe used the following email accounts: r00t3dx@hotmail.com and syzt3m@gmail.com.

9. SoBe used the following user name: Serlissmc.

10. SoBe used the following other nicknames: ebos, shksobe, syzt3m, and vapidz.

INTERNET SERVICE PROVIDERS

11. Many individuals and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs").

//

12. ISPs offer their customers access to the Internet using telephone or other telecommunications lines. ISPs provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers. ISPs remotely store electronic files on their customers' behalf, and may provide other services unique to each particular ISP.

America Online

13. America Online, Inc. ("AOL") was an ISP headquartered in Dulles, Virginia.

14. In addition to Internet access, Internet e-mail accounts, and remote storage of electronic files, AOL also offered its customers a free online service called AOL Instant Messenger ("AIM"), which allowed users to communicate in real time.

INTERNET HOSTING COMPANIES

15. Internet hosting companies provide individuals or businesses with large scale access to the Internet through the use of computers large enough to be capable of providing one or more services to other computers on the Internet. These large computers are commonly referred to as "servers" or "boxes." Use of a server is often combined with access to a larger network of computers. The services of Internet hosting companies enable customers to conduct activity on the Internet, such as operate web sites, administer networks, or run email systems.

EasyDedicated

16. EasyDedicated International B.V. was an Internet hosting company located in Amsterdam, Netherlands.

//.

17. EasyDedicated provided its customers with large scale Internet connectivity, access to networks of computers, and the use of servers and other hardware.

18. EasyDedicated provided these services to customers residing outside of the Netherlands through its online business, EasyDedicated.com.

FDCServers

19. FDCServers was an Internet hosting company located in Chicago, Illinois.

20. FDCServers provided its customers with large scale Internet connectivity, access to networks of computers, and the use of servers and other hardware.

The Planet

21. The Planet was an Internet hosting company located in Dallas, Texas.

22. The Planet provided its customers with large scale Internet connectivity, access to networks of computers, and the use of servers and other hardware.

Sago Networks

23. Sago Networks was an Internet hosting company located in Tampa, Florida.

24. Sago Networks provided its customers with large scale Internet connectivity, access to networks of computers, and the use of servers and other hardware.

ADVERTISING SERVICE COMPANIES

25. Online merchants often hire advertising service companies to send traffic to their web sites. These advertising service companies in turn maintain advertising affiliate programs, whereby

an individual, typically someone who operates a web site, is hired to place on the website certain links advertising the merchant's product or business, and is then compensated based upon the number of visitors to the website that click on that link.

26. Some advertising service companies with multiple online merchant clients compensate their affiliates each time a type of software known as "adware" is successfully installed on a visitor's computer. Adware collects information about an Internet user in order to display advertisements in the user's Web browser based upon information it collects from the user's browsing patterns.

27. Adware is usually installed on an Internet user's computer only upon notice or if the user performs some action, like clicking a button, installing a software package, or agreeing to enhance the functionality of a Web browser by adding a toolbar or additional search box.

28. Advertising service companies typically identify their affiliates by some type of identification number or code that is included in the adware; they then tally up the number of installs and periodically pay the affiliate based upon a percentage of the number of installs, usually through Paypal, direct bank deposit, or by check mailed to the affiliate.

Gammacash

29. Gamma Entertainment, Inc. was an advertising service company located in Quebec, Canada.

30. Gamma Entertainment was associated with the web sites www.toolbarcash.com, www.gammacash.com, and www.xxxtoolbar.com. These web sites were advertising service web sites which offered advertising affiliate programs pertaining to the installation of

adware.

31. Gamma Entertainment compensated its affiliates for each installation of adware made with notice to and/or consent from any Internet user.

LOUDcash

32. CDT Inc. was an advertising service company located in Quebec, Canada. CDT was associated with advertising service web sites called www.loudmarketing.com and www.loudcash.com. Through these web sites, CDT offered an advertising affiliate program called "LOUDcash" or "lc."

33. LOUDcash compensated its affiliates for each installation of adware made with notice to and/or consent from any Internet user.

34. In or about April 2005, 180solutions, an advertising service company located in Bellevue, Washington, acquired CDT, Inc. As a result, LOUDcash became a subsidiary of a company called Zango Nevada LLC and was renamed ZangoCash.

PAYPAL

35. Paypal, Inc. was an online payment solutions company located in San Jose, California.

36. Paypal used a website located at www.paypal.com to enable any individual or business with an e-mail address to securely, easily and quickly send and receive payments online. Paypal's service built on the existing financial infrastructure of bank accounts and credit cards to create a real time payment solution.

CHINA LAKE NAVAL AIR FACILITY

37. The Weapons Division of the United States Naval Air Warfare Center was located in China Lake, California.

38. This federal government facility maintained a computer network for its exclusive use called chinalake.navy.mil.

39. The Weapons Division used this network in furtherance of national defense.

DEFENSE INFORMATION SYSTEM AGENCY

40. The Defense Information Systems Agency ("DISA") was part of the United States Department of Defense ("DOD"), and was headquartered in Falls Church, Virginia.

41. DISA was a combat support agency responsible for planning, engineering, acquiring, fielding, and supporting global network based solutions to serve the needs of the President, the Vice-President, the Secretary of Defense, and various other DOD components, under all conditions of peace and war.

42. DISA maintained and exclusively used a computer network called disa.mil in furtherance of its national defense mission.

NEXUS TO COMMERCE

43. The computers belonging to EasyDedicated, FDCServers, Sago Networks, and The Planet were used in interstate and foreign commerce and communication.

COMPUTER TERMINOLOGY

Bot

44. 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 Internet Relay Chat ("IRC") servers. The term "bot" also refers to computers that have been infected with a program used to control or launch distributed denial of service attacks against other computers.

Botnet

45. A "botnet" is typically a network of computers infected with bots that are used to control or attack computer systems. Botnets are often created by spreading a computer virus or worm that propagates throughout the Internet, gaining unauthorized access to computers on the Internet, and infecting the computer with a particular bot program. The botnet is then controlled by a user, often through the use of a specified channel on Internet Relay Chat. 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 to launch distributed denial of service attacks.

Clickers

46. "Clickers" refer to malicious code or exploits that redirect victim machines to specified web sites or other Internet resources. Clickers can be used for advertising purposes or to lead a victim computer to an infected resource where the machine will be attacked further by other malicious code.

Distributed Denial of Service Attack

47. A distributed denial of service attack or "DDOS attack" is a type of malicious computer activity where 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.

Domain Name Server

48. A "domain" is a set of subjects and objects on the Internet which share common security policies, procedures, and rules, and are managed by the same management system. A "domain name" identifies where on the World Wide Web the domain is located. A "domain name server" or "DNS" translates or maps domain names to Internet Protocol ("IP") addresses and vice versa. Domain name servers maintain central lists of domain names/IP addresses, translate or map the domain names in an Internet request, and then send the request to other servers on the Internet until the specified address is found.

Exe

49. "Exe" is short for "executable" or ".exe" or executable file, and refers to a binary file containing a program that is ready to be executed or run by a computer. Hackers many times refer to their malicious programs or code as ".exe" or "exe." For example Hacker1 may ask Hacker2, "Did your exe spread over the network?"

Exploit

50. An "exploit" is computer code written to take advantage of a vulnerability or security weakness in a computer system or software.

Internet Protocol Address

51. An "Internet protocol address" or "IP address" is a unique numeric address used by computers on the Internet. An IP address is designated by a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every

computer connected 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 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.

Internet Relay Chat

52. Internet Relay Chat ("IRC") is a network of computers connected through the Internet that allows users to communicate with others in real time text (known as "chat"). IRC users utilize specialized client software to use the service and can access a "channel" which is administered by one or more "operators" or "ops." IRC channels are sometimes dedicated to a topic and are identified by a pound sign and a description of the topic such as "#miamidolphins." IRC channels are also used to control botnets that are used to launch DDOS attacks, send unsolicited commercial email, and generate advertising affiliate income.

Internet Relay Chat Daemon

53. Internet Relay Chat Daemon ("IRCD") is a computer program used to create an IRC server on which people can chat with each other via the Internet.

Port

54. A "port" is a process that permits the operating system of a computer to know what to do with incoming traffic. A computer does not have physical ports. Rather, a port is a process that permits the computer to process information as it arrives at the computer. All incoming traffic has a "header" as well as its

content. Part of the header information identifies the port to which the incoming information is addressed. For example, Port 80 is, by convention, website traffic. As a packet of information is received, the computer operating system notes that it is addressed to Port 80 and sends the packet to the web operating software. Similarly, Port 25 is for incoming e-mail. When the operating system sees a packet of information addressed to Port 25, it directs the packet to the e-mail software.

Root/Administrative Privileges

55. Also known as "superuser" privileges, a user that has "root" or "administrator" status on a system has access to the system at a level sufficient to allow the user to make changes to the system in ways that a regular user accessing the system cannot.

Server

56. A "server" or "box" is a centralized computer that provides services for other computers connected to it via a network. The other computers attached to a server are sometimes called "clients." In a large company, it is common for individual employees to have client computers on their desktops. When the employees access their email, or access files stored on the network itself, those files are pulled electronically from the server where they are stored, and are sent to the client's computer via the network. In larger networks, it is common for servers to be dedicated to a single task. For example, a server that is configured so that its sole task is to support a World Wide Web site is known simply as a "web server." Similarly, a server that only stores and processes email is known as a "mail server."

//

Spam & Proxies

57. "Spam" refers to unsolicited commercial email. "Spamming" refers to the mass or bulk distribution of unsolicited commercial email.

58. Some spammers use software to extract and harvest target screen names and email addresses from newsgroups, chat rooms, email servers, and other areas of the Internet. Others simply enlist the "bulk e-mail services" of foreign or overseas companies.

59. Often spammers use computers infected with malicious code and made vulnerable to subsequent unauthorized access by routing spam through the victim computer in order to mask their originating email and IP address information. In this way, the infected computer serves as a "proxy" for the true spammer.

SynFlood

60. A "synflood" is a type of DDOS attack where 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 causes the victimized computer to use all of its resources to respond to the requests and renders it unable to handle legitimate traffic.

Toolbar

61. A "toolbar" is a row or column of on-screen buttons used to activate functions in the application. Toolbars used as adware or malicious code often cause advertisements to pop up on the

infected user's computer.

Trojan

62. A "Trojan" or "Trojan Horse" is a malicious program that is disguised as a harmless application or is secretly integrated into legitimate software. A Trojan is typically silently installed and hides from the user. Although typically not self-replicating, additional components can be added to a Trojan to enable its propagation. A Trojan often allows a malicious attacker to gain unauthorized remote access to a compromised computer, infect files, or damage systems.

Uniform Resource Locator ("URL")

63. "Uniform Resource Locator" or "URL" is the unique address which identifies a resource on the Internet for routing purposes, such as http://www.cnn.com.

Worm

64. A "worm" is a program that replicates itself over a computer network and usually performs malicious actions, such as exhausting the computer's resources and possibly shutting the system down. Unlike a virus, a worm needs little or no human assistance to spread.

//

//

//

//

//

//

//

//

COUNT ONE

[18 U.S.C. § 371]

65. The Grand Jury hereby repeats and re-alleges all of the introductory allegations set forth in paragraphs 1 through 64 of this Indictment.

OBJECTS OF THE CONSPIRACY

66. Beginning at least as early as June 25, 2004, and continuing through at least as late as September 15, 2004, in Los Angeles County, within the Central District of California, and elsewhere, defendant JEANSON JAMES ANCHETA, and others known and unknown to the Grand Jury, knowingly conspired, confederated, and agreed with each other:

a. To knowingly cause the transmission of a program, information, code and command, and as a result of such conduct, intentionally cause damage without authorization to a computer used in interstate and foreign commerce and communication, and cause loss during a one-year period aggregating at least $5,000 in value, in violation of 18 U.S.C. §§ 1030(a)(5)(A)(i), 1030(a)(5)(B)(i), and 1030(b); and

b. To access without authorization a computer used in interstate and foreign commerce and communication, and intentionally initiate the transmission from and through that computer of multiple commercial electronic mail messages that affect interstate and foreign commerce, in violation of 18 U.S.C. §§ 1037(a)(1), 1037(b)(2)(A), and 1037(b)(2)(F).

MEANS BY WHICH THE CONSPIRACY WAS TO BE ACCOMPLISHED

67. The objects of the conspiracy were to be accomplished as follows:

68. ANCHETA would obtain access to a server from an Internet hosting company.

69. ANCHETA would use the server as an IRC server by running an IRCD.

70. ANCHETA would create a channel in IRC which he controlled.

71. ANCHETA would develop a worm which would cause infected computers, unbeknownst to the users of the infected computers, to:

a. report to the IRC channel he controlled;

b. scan for other computers vulnerable to similar infection; and

c. succumb to future unauthorized accesses, including for use as proxies for spamming.

72. ANCHETA would use the server to disseminate the worm, infect vulnerable computers connected to the Internet, and cause thousands of victim computers per day to report to the IRC channel he controlled on the server.

73. ANCHETA would then advertise the sale of bots for the purpose of launching DDOS attacks or using the bots as proxies to send spam.

74. ANCHETA would sell up to 10,000 bots or proxies at a time.

75. ANCHETA would discuss with purchasers the nature and extent of the DDOS or proxy spamming they were interested in conducting, and recommend the number of bots or proxies necessary to accomplish the specified attack.

76. ANCHETA would set the price based upon the number of bots or proxies purchased.

77. For an additional price, ANCHETA would provide the purchaser with worm or exe, and set up or configure it for the particular purchaser's use so that it would cause the purchased bots or proxies to spread or propagate.

78. For an additional price, ANCHETA would create a separate channel on his IRC server, rally or direct the purchased bots to that channel, and grant the purchaser access to the IRC server and control over that channel.

79. ANCHETA would accept payments through Paypal.

80. ANCHETA would either describe, or direct the purchaser to describe, the nature of the transaction in Paypal as "hosting" or "web hosting" or "dedicated box" services, in order to mask the true nature of the transaction.

81. Once he received payment, ANCHETA would set up or configure the purchased botnet for the purchaser, test the botnet with the purchaser in order to ensure that DDOS attacks or proxy spamming would be successfully carried out, or advise the purchaser about how to properly maintain, update, and strengthen the purchased botnet.

OVERT ACTS

82. In furtherance of the conspiracy, and to accomplish the objects of the conspiracy, defendant JEANSON JAMES ANCHETA and others known and unknown to the Grand Jury, committed various overt acts in Los Angeles County, within the Central District of California, and elsewhere, including the following:

Opening for Business

83. On or about June 25, 2004, ANCHETA leased a server from Sago Networks.

84. In or about early July 2004, ANCHETA ran an IRCD so that he could use the server he leased from Sago Networks as an IRC server.

85. In or about early July 2004, ANCHETA modified for his own purposes a Trojan called "rxbot," a malicious code known to provide a nefarious computer attacker with unauthorized remote administrative level control of an infected computer by using commands sent over IRC.

86. In or about early July 2004, ANCHETA used the modified rxbot to scan for and exploit vulnerable computers connected to the Internet, causing them to rally or be directed to a channel in IRC which he controlled, to scan for other computers vulnerable to similar infection, and to remain vulnerable to further unauthorized access.

87. In or about early July 2004, ANCHETA created a channel in IRC called #botz4sale.

88. In or about early July 2004, ANCHETA inserted a link in IRC channel #botz4sale to an advertisement and price list pertaining to the sale of bots and proxies.

Sale to Circa

89. On or about July 10, 2004, during a chat in IRC, an unindicted co-conspirator using the nickname "circa" asked ANCHETA to sell her 10,000 bots so that she could "mail from the proxies."

90. On or about July 10, 2004, during a chat in IRC, ANCHETA asked circa how much she made "off proxies," to which circa responded, "I make pretty good money."

91. Between on or about July 10, 2004 and August 7, 2004, ANCHETA sold bots to circa and received payments from circa via

Paypal totaling approximately $400.

Sale to KiD

92. On or about July 19, 2004, during a chat in IRC, an unindicted co-conspirator using the nickname KiD told ANCHETA that he needed a more effective worm to expand his existing 2,500-strong botnet.

93. On or about July 20, 2004, ANCHETA sold the worm he had used to create the bots and proxies advertised on #botz4sale to KiD, and received payment for the worm through Paypal.

94. On or about July 22, 2004, during a chat in IRC, KiD asked ANCHETA "wats [sic] the best ddos command" for the worm KiD had purchased from ANCHETA.

95. On or about July 22, 2004, during a chat in IRC, ANCHETA told KiD that he had more than 40,000 bots for sale, commenting, "more than I can handle, I can't even put them all online because I don't have enough servers, so I'm not even sure how many I got."

Sale to zxpL

96. On or about July 23, 2004, during a chat in IRC, ANCHETA told an unindicted co-conspirator using the nickname "zxpL" that his worm caused 1,000 to 10,000 new bots to join his botnet over the course of only three days.

97. On or about July 23, 2004, during a chat in IRC, zxpL told ANCHETA that his own server could hold only 7,000 bots, and asked ANCHETA to conduct a synflood DDOS attack against an IP address belonging to King Pao Electronic Co., Ltd. in Taipei, Taiwan, which zxpL identified for ANCHETA.

98. On or about July 23, 2004, during a chat in IRC, zxpL offered to buy ANCHETA's worm with advertising affiliate proceeds

zxpL had generated using his own botnet.

99. On or about July 24, 2004, during a chat in IRC, zxpL again asked ANCHETA to conduct a synflood DDOS attack, this time against an IP address belonging to Sanyo Electric Software Co., Ltd. in Osaka, Japan, which zxpL identified for ANCHETA.

100. On or about July 26, 2004, zxpL asked ANCHETA to create a separate IRC channel for the bots he would purchase from ANCHETA.

101. By on or about August 2, 2004, ANCHETA sold an exe and 1,500 bots to zxpL and received payment through Paypal, bringing the number of bots available to zxpL for DDOS attacks to at least 8,500.

102. On or about August 3, 2004, during a chat in IRC, zxpL told ANCHETA, "ur [your] bot spreads uber fast."

Improving the Business

103. In or about August 2004, ANCHETA updated his advertisement to increase the price of bots and proxies, to limit the purchase of bots to 2,000 "due to massive orders," and to warn, "I am not responsible for anything that happens to you or your bots after you see your amount of bots you purchased in your room [IRC channel]."

Sales to Daytona and MLG

104. On or about August 6, 2004, ANCHETA sold an exe and 250 bots to an unindicted co-conspirator using the nickname "Daytona," and received payment through Paypal.

105. On or about August 6, 2004 through August 9, 2004, during several chats in IRC, ANCHETA educated Daytona about how to maintain and use the bots Daytona had purchased from ANCHETA.

//

106. On or about August 9, 2004, during chats in IRC, Daytona asked ANCHETA to sell Daytona additional bots, explaining, "I need the bots bad . . . I need the bots . . . I need them bots . . . send asap."

107. On or about August 9, 2004, ANCHETA sold an additional 400 bots to Daytona, and received payment through Paypal.

108. The next day, on or about August 10, 2004, Daytona introduced ANCHETA to another potential buyer, an unindicted co-conspirator using the nickname "MLG".

109. On or about August 10, 2004, during a chat in IRC, MLG told ANCHETA that he needed the bots to launch DDOS attacks, explaining, it "just doesn't feel the same unless ya do 'em yourself. . :)[smile]."

110. On or about August 10, 2004, Daytona gave MLG 100 of the bots Daytona had purchased from ANCHETA.

111. On or about August 10, 2004, MLG sent ANCHETA payment through Paypal.

112. On or about August 10, 2004, ANCHETA gave 250 bots to Daytona, who kept 150 of them as payment from MLG for brokering the sale between ANCHETA and MLG.

<u>Sale to Teh1</u>

113. On or about July 13, 2004, during a chat in IRC, unindicted co-conspirator "Teh1" asked ANCHETA to sell him a worm or exe that would cause advertising affiliate adware to surreptitiously install on bots in a 2,000 strong botnet.

114. On or about July 13, 2004, during a chat in IRC, ANCHETA agreed to give Teh1 the requested exe, told Teh1, "Keep making your bots download my .exe" until Teh1's botnet generated at least $50

in proceeds from surreptitious advertising affiliate adware installs, and instructed Teh1 to then transfer the $50 to ANCHETA as payment for the exe.

115. Between on or about July 14, 2004 and on or about August 12, 2004, ANCHETA and Teh1 continued to negotiate the sale of the exe.

116. On or about August 12, 2004, ANCHETA sold an exe to Teh1, and received payment through Paypal.

Sale to Sploit

117. On or about August 21, 2004, ANCHETA sold $300 worth of bots to an unindicted co-conspirator using the nickname "Sploit".

118. During a subsequent chat in IRC, Sploit explained to ANCHETA that he needed to purchase bots for spamming because he owned a data center in Japan that he used for "100% spam," commenting to ANCHETA, "I can mail from those to the U.S., plus they get decent speeds."

Sales to O_2iginal

119. On or about August 21, 2004, during a chat in IRC, ANCHETA told an unindicted co-conspirator using the nickname "o_2riginal" that he was hosting "around 100k bots total," that in a week and a half 1,000 of his bots scanned and infected another 10,000, and that his botnet would be bigger if he had not used some himself for "ddosing."

120. On or about August 21, 2004, during a chat in IRC, o_2riginal warned ANCHETA that he should make sure "to filter out shit though like .gov and .mils" after his bots scanned and infected other computers.

//

121. On or about August 21, 2004, during a chat in IRC, o_2riginal told ANCHETA that o_2riginal was a "big spam[mer]," that he "got all this work but not enough resources," that he wanted to buy 1,000 bots "for packeting and a fucking proxy subscription," and asked, "If I use these bots as proxies will they go down easily?", to which ANCHETA responded, "on my bots, yeah, fo shizzle."

122. On or about August 21, 2004, during a subsequent chat in IRC, ANCHETA offered to sell o_2riginal 7,000 proxies, explaining that the life of the proxies "depends on how long it takes the server to ban the proxies that ur mailing through."

123. On or about August 21, 2004, ANCHETA sold o_2riginal 3,000 proxies, and received payment through Paypal.

124. On or about August 23, 2004, ANCHETA sold o_2riginal 2,000 bots and an exe that would cause the purchased bots to spread or propagate, and received payment through Paypal.

125. From on or about August 23, 2004 through September 15, 2004, during chats in IRC, ANCHETA advised 0_2riginal how to maintain, update, and strengthen the purchased botnet.

Sale to Seminole Pride

126. On or about August 23, 2004, an unindicted co-conspirator using the nickname "Seminole Pride" sent ANCHETA payment through Paypal for the purchase of 100 bots and the exe that would cause the purchased bots to spread or propagate.

127. On or about August 24, 2004, Seminole Pride provided ANCHETA with the server name "irc.dsstrust.com" and the channel "#floodz" so that ANCHETA could load the exe and rally or direct the purchased bots to that channel.

128. On or about August 24, 2004, ANCHETA completed the sale to Seminole Pride by loading the exe and rallying or directing the purchased bots to IRC channel #floodz.

Sale to Longwordus

129. On or about September 15, 2004, during a chat on AIM, an unindicted co-conspirator using the nickname "Longwordus" asked ANCHETA to purchase 1,000 bots and an exe to cause the bots to spread or propagate.

130. On or about September 15, 2004, ANCHETA sold 1,000 bots and exe to Longwordus, and received payment through Paypal.

131. On or about September 15, 2004, ANCHETA set up or configured the exe for Longwordus and helped him test the purchased botnet.

Sale to a Confidential Source

132. On or about August 4, 2004, during a chat on AIM, ANCHETA told a confidential source that he earned $1,000 in two weeks by selling bots and proxies, and that he would be willing to sell some to the confidential source.

133. On or about August 13, 2004, during a chat on AIM, when the confidential source told ANCHETA that he wanted to purchase bots to conduct DDOS attacks against some web sites, ANCHETA inquired whether the confidential source knew "rx" and understood how to launch "rx dDOS attacks."

134. On August 24, 2004, when the confidential source, posing as a different user, contacted ANCHETA over AIM and asked "to buy some bots for proxys," ANCHETA confirmed his ability to do so and asked the confidential source to contact him "in a few hours."

135. On August 25, 2004, when the confidential source, posing as yet another user, contacted ANCHETA over AIM and asked to purchase a large botnet consisting of 20,000 compromised computers with good attack power and the ability to send spam, ANCHETA told the confidential source that he would be willing to sell only up to 2,000 bots.

136. On August 25, 2004, during a chat on AIM, when the confidential source asked ANCHETA whether 2,000 bots would be "enough to drop a site," ANCHETA confirmed that 2,000 bots would be capable of launching various types of DDOS attacks, including a synflood.

137. On August 25, 2004, during a chat on AIM, when the confidential source specifically explained to ANCHETA that he needed a botnet strong and stable enough to launch a synflood DDOS attack against a business competitor operating a web site at 500 megabits per second, ANCHETA confirmed again that 2,000 of his bots would be "plenty" to take down that specific site.

138. On or about August 31, 2004, ANCHETA sold the confidential source 2,000 bots, the exe to cause the bots to spread, and space on ANCHETA's IRC server to host the purchased botnet, receiving payment through Paypal.

139. On or about September 1, 2004, during a chat in IRC, ANCHETA sent the confidential source a file to download the purchased exe, and requested that the confidential source run the exe to enable the particular IRC channel ANCHETA had set up for the confidential source to accept bots.

//

//

140. On or about September 1, 2004, during a chat in IRC, ANCHETA accessed his botnet and issued commands to rally or direct 2,000 bots to join the particular IRC channel ANCHETA had set up for the confidential source.

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

COUNT TWO

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

141. The Grand Jury hereby repeats and re-alleges all of the introductory allegations set forth in paragraphs 1 through 64, as well as paragraphs 66 through 88 and 96 through 103 of this Indictment.

142. Beginning on or about July 23, 2004 and continuing through on or about August 3, 2004, in Los Angeles County, within the Central District of California, and elsewhere, defendant JEANSON JAMES ANCHETA attempted to knowingly cause the transmission of a program, information, code and command, and as a result of such conduct, intentionally cause damage without authorization to a computer used in interstate and foreign commerce and communication, namely, defendant JEANSON JAMES ANCHETA supplied an unindicted co-conspirator using the nickname zxpL with malicious computer code and unauthorized access to 1,500 compromised computers in order to launch distributed denial of service attacks against protected computers using IP addresses 210.209.57.1 and 219.106.106.37 and belonging to King Pao Electronic Co., Ltd. and Sanyo Electric Software Co., Ltd., respectively, which, as a result of such conduct, would have caused, if completed, loss during a one-year period aggregating at least $5,000 in value.

//

//

//

//

//

//

COUNT THREE

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

143. The Grand Jury hereby repeats and re-alleges all of the introductory allegations set forth in paragraphs 1 through 64, as well as paragraphs 66 through 88, 103, and 132 through 140 of this Indictment.

144. Beginning on or about August 25, 2004 and continuing through on or about September 1, 2004, in Los Angeles County, within the Central District of California, and elsewhere, defendant JEANSON JAMES ANCHETA attempted to knowingly cause the transmission of a program, information, code and command, and as a result of such conduct, intentionally cause damage without authorization to a computer used in interstate and foreign commerce and communication, namely, defendant JEANSON JAMES ANCHETA supplied a confidential source with malicious computer code, unauthorized access to 2,000 compromised computers, and use of an IRC server, all in order to launch distributed denial of service attacks against protected computers operating a web site at 500 megabits per second belonging to a business competitor of the confidential source, which, as a result of such conduct, would have caused, if completed, loss during a one-year period aggregating at least $5,000 in value.

//

//

//

//

//

//

//

COUNT FOUR

[18 U.S.C. § 371]

145. The Grand Jury hereby repeats and re-alleges all of the introductory allegations set forth in paragraphs 1 through 64, as well as paragraphs 98, 113, and 114 of this Indictment.

OBJECTS OF THE CONSPIRACY

146. Beginning at least as early as August 2004 and continuing through at least as late as August 2005, in Los Angeles County, within the Central District of California, and elsewhere, defendant JEANSON JAMES ANCHETA, and others known and unknown to the Grand Jury, knowingly conspired, confederated, and agreed with each other:

a. To knowingly cause the transmission of a program, information, code and command, and as a result of such conduct, intentionally cause damage without authorization to a computer involved in interstate and foreign commerce and communication, and cause loss aggregating more than $5,000 in a one-year period, and damage affecting a computer system used by and for a government entity in furtherance of the administration of justice, national defense, and national security, all in violation of 18 U.S.C. §§ 1030(a)(5)(A)(i), 1030(a)(5)(B)(i), 1030(a)(5)(B)(v), and 1030(b); and

b. To knowingly and with intent to defraud, access a computer used in interstate and foreign commerce and communication without authorization, and by means of such conduct, further the intended fraud and obtain something of value, in violation of 18 U.S.C. §§ 1030(a)(4) and 1030(b).

//

MEANS BY WHICH THE CONSPIRACY WAS TO BE ACCOMPLISHED

147. The objects of the conspiracy were to be accomplished as follows:

148. ANCHETA and an unindicted co-conspirator using the nickname "SoBe" would obtain access to servers from Internet hosting companies.

149. ANCHETA and SoBe would use servers to which they had access as IRC servers by running IRCDs.

150. ANCHETA and SoBe would create channels in IRC which they controlled.

151. ANCHETA and SoBe would enroll as affiliates of advertising service companies and obtain affiliate identification numbers for the purpose of receiving compensation for adware installations.

152. ANCHETA and SoBe would create clickers; namely, they would modify without permission the adware they obtained from the advertising service companies to enable the adware to be surreptitiously installed without notifying, or requiring any action from, a computer's user, but nonetheless appear to the advertising service companies as legitimately installed.

153. ANCHETA and SoBe would use other servers to which they had access as servers hosting malicious adware or clickers.

154. ANCHETA and SoBe would cause the transmission of malicious code to computers connected to the Internet, causing the infected computers to report to an IRC channel controlled by ANCHETA and SoBe, thereby creating a botnet.

155. ANCHETA and SoBe would cause infected computers in the botnet to be redirected to one of their adware servers, where files

containing components of a Trojan horse program would download onto the infected computers, causing the surreptitious installation of adware.

156. ANCHETA and SoBe would cause the advertising affiliate companies whose adware would be surreptitiously installed on an infected computer to be notified of that instance of installation, and to credit one of their affiliate identification numbers for that installation.

157. ANCHETA and SoBe would receive periodic payments from advertising service companies based upon the number of installations of adware that were credited to them.

158. To avoid detection by network administrators, security analysts, or law enforcement, and thereby maintain the integrity of the scheme, ANCHETA and SoBe would use IRC channel topic commands to vary the download times and rates of adware installations so that the installations would appear to be legitimate web traffic to anyone that may be watching.

159. When a company hosting a particular adware server grew suspicious of or discovered the malicious activity, ANCHETA and SoBe would cause infected computers residing on IRC servers they controlled, or to which they had access, to be redirected to another adware server they controlled, or to which they had access, so as to further maintain the integrity and success of the scheme.

160. ANCHETA would transfer a portion of the payments he received from advertising service companies to SoBe as a fee for maintaining the botnet and adware servers.

//

//

OVERT ACTS

161. In furtherance of the conspiracy, and to accomplish the objects of the conspiracy, defendant JEANSON JAMES ANCHETA and others known and unknown to the Grand Jury, committed various overt acts in Los Angeles County, within the Central District of California, and elsewhere, including the following:

162. On or about August 13, 2004, ANCHETA transferred $114.00 to Sago Networks through Paypal as payment for access to a server.

163. On or about September 3, 2004, ANCHETA transferred $100.00 to Sago Networks through Paypal as payment for access to a server.

164. On or about September 21, 2004, during a chat on AIM, ANCHETA told another AIM user who had offered to install ANCHETA's clickers on bots in exchange for a percentage of any advertising affiliate payment generated, "i pay sherby $500 month to do my clicker everyday as topic for 30 min but he has a lot of bots ... i mean SOBE."

165. On or about September 27, 2004, ANCHETA transferred $200.09 from his Wells Fargo Bank account to The Planet as payment for access to a server.

166. On or about October 8, 2004, ANCHETA received $2,305.89 from LOUDcash through Paypal.

167. On the same day, on or about October 8, 2004, ANCHETA transferred $120 to SoBe through Paypal.

168. On or about October 5, 2004, during a chat on AIM, ANCHETA educated SoBe about how to avoid detection by network administrators, security analysts, or law enforcement, explaining, among other things, "try and limit yourself from logging into your

bots unless its very important because that's how it gets sniffed," "if you do login into your bots don't ever [use] your real handle," and if "authorities or anything" find "the box," "just ignore and notify me."

169. On or about October 5, 2004, during a chat on AIM, ANCHETA gave SoBe the operator password to the IRC channel #syzt3m#.

170. On or about October 5, 2004, during a chat on AIM, ANCHETA asked SoBe, "when do you want to start doing the lc [LOUDcash] stuff again. . .i'm still waiting for lc [LOUDcash] to fucking pay. . .tomorrow they should pay since its the 6th."

171. On or about October 17, 2004, during a chat on AIM, while discussing with SoBe clicker install statistics, ANCHETA stated that he was receiving affiliate credit for at least 1,000 clickers per day, commenting, "i'm averaging an extra 2-3 buffalo.edu per 30 minutes with this forbot hehe."

172. On or about October 17, 2004, during a chat on AIM, after learning from SoBe that a server they controlled, or to which they had access, "hit new high max this morning," that SoBe believed they would need access to another server soon, and that SoBe would need help in moving some of the botnet to a new server, ANCHETA replied, "i dont care ur helping me im helping you its all good."

173. On or about October 17, 2004, during a chat on AIM, ANCHETA reassured SoBe, explaining "fbi dont bust ya for having bots. . .its how you use them. . .i mean think about it, a company that makes thousands a day and you crippled it just for a day they lose lots and not just affecting that site your affecting many others on that box . . .haha many ways of killing a box without

ddos -=)."

174. On or about October 17, 2004, during a chat on AIM, ANCHETA instructed SoBe to "switch to lc [LOUDcash]," to which SoBe responded, "i forgot actually . . .damn, that was almost an hour. . .the reason why i dont like to do both [affiliate programs] . . .is than [sic] i would be paying them so much."

175. On or about October 18, 2004, ANCHETA transferred $65.00 to Sago Networks through Paypal as payment for access to a server.

176. On or about October 20, 2004, ANCHETA deposited a $3,034.61 check from Gammacash into his Wells Fargo Bank account.

177. On or about October 21, 2004, during a chat on AIM, when SoBe complained that "there werent a lot of bots," ANCHETA told SoBe to "stay in the server" and that ANCHETA would "restart the box first thing tomorrow."

178. On or about October 21, 2004, during a chat on AIM, ANCHETA discussed with SoBe how to change the topic in the IRC channel to maximize the number of bots successfully redirected to the adware servers without detection.

179. On or about October 24, 2004, during a chat on AIM, ANCHETA told SoBe, "if you wanna keep seeing the money coming lets keep the bot talking to nothing," explaining, "there are tons of admins [network administrators] out there, thats why i tell everyone i have no bots."

180. On or about October 24, 2004, during a chat on AIM, ANCHETA and SoBe discussed their affiliate earnings, ANCHETA predicted that SoBe would make "2.2gs" by the end of the month, and when SoBe asked, "I wonder how long itll last," ANCHETA responded, "as long as everything is [on the "down low" or undiscovered] im

estimating 6 more months to 8 months, hopefully a year."

181. On or about October 30, 2004, during a chat on AIM, ANCHETA told SoBe he was setting the topic in IRC to LOUDcash, namely, that ANCHETA would redirect the bots in the IRC channel to navigate to the adware server where LOUDcash clickers would surreptitiously install onto the bots.

182. On or about October 30, 2004, during a chat on AIM, ANCHETA discussed with SoBe the money they were making, commenting "its easy like slicing cheese," to which SoBe later responded, "I just hope this lc [LOUDcash] stuff lasts a while so I don't have to get a job right away."

183. On or about October 31, 2004, during a chat on AIM, ANCHETA mentioned to SoBe, "you did good this month," predicted that SoBe would make over $1,000 for the month, and instructed SoBe to upgrade his Paypal account so that he could receive a payment in an amount over $1,000.

184. On or about October 31, 2004, during a chat on AIM, SoBe told ANCHETA, "hey btw [by the way] there are gov/mil on the box if you want to get rid of them," to which ANCHETA responded "rofl [rolling on the floor laughing]."

185. In or about November 2004, ANCHETA leased a server located at FDCServers.

186. On or about November 2, 2004, ANCHETA transferred $187.00 from his Wells Fargo Bank account to The Planet as payment for access to a server.

187. On or about November 5, 2004, ANCHETA deposited a $3,970.91 check from Gammacash into his Wells Fargo Bank account.

//

188. On or about November 9, 2004, ANCHETA obtained access to a server located at EasyDedicated.

189. On or about November 10, 2004, during a chat on AIM, when SoBe told ANCHETA that a large number of bots from uncc.edu were reporting to an IRC channel they controlled, or to which they had access, ANCHETA warned SoBe "if you do it too much you will get caught up one time or another."

190. On or about November 12, 2004, during a chat on AIM, SoBe told ANCHETA, "we hit 49.990k this morning, usually the box peaks at 50000," to which ANCHETA responded, "im getting another box. . .i suggest u do too."

191. On or about November 12, 2004, during a chat on AIM, ANCHETA asked SoBe to remind him which email account SoBe was using at Paypal so that ANCHETA could pay him from the affiliate proceeds ANCHETA was expecting to receive shortly.

192. On or about November 16, 2004, ANCHETA received $1,263.73 from LOUDcash through Paypal.

193. On the same day, or about November 16, 2004, ANCHETA transferred $1,100 to SoBe through Paypal.

194. On or about November 19, 2004, ANCHETA deposited a $4,044.26 check from Gammacash into his Wells Fargo Bank account.

195. Or about November 19, 2004, during a chat on AIM, ANCHETA told SoBe that he had set up a server "just as a distraction for the fbi to see that im running legal network."

196. On or about November 20, 2004, during a chat on AIM, ANCHETA told SoBe, "hey bro try to find me a west coast datacenter that allows ircd."

//

197. On or about November 20, 2004, during a chat on AIM, ANCHETA told SoBe "i hope the box dont get reported again, I ddosed with my bots on there, i needed the extra power, it wont get reported though since its a new .exe."

198. On or about November 20, 2004, during a chat on AIM, ANCHETA told SoBe that he would change the topic in the IRC channel to redirect the bots to a different adware server and monitor the channel for an hour or so while SoBe was unavailable to do so.

199. On or about November 20, 2004, during a chat on AIM, while discussing their affiliate earnings, ANCHETA told SoBe, "my average spending is $600 a week, every friday I buy new clothes and every week I buy new parts for my car."

200. On or about November 23, 2004, ANCHETA transferred $149.00 from his Wells Fargo Bank account to FDCServers as payment for access to a server.

201. On or about November 24, 2004, ANCHETA caused SoBe to obtain access for them to a server from Sago Networks.

202. On or about November 27, 2004, during a chat on AIM, ANCHETA taught SoBe how to run IRCD, configure, and set root/administrator privileges and passwords on the new server SoBe had leased from Sago Networks.

203. On or about November 28, 2004, during a chat on AIM, ANCHETA told SoBe that one of their adware servers was flooded and instructed SoBe to set more than one topic in IRC for a few hours to simultaneously direct the bots to multiple adware servers to correct the problem.

204. On or about December 7, 2004, during a chat on AIM, ANCHETA agreed with SoBe that he should log into the IRC channel

and improve the "scanners."

205. On or about December 7, 2004, during a chat on AIM, ANCHETA warned SoBe to use more innocuous, common sounding names like "imports" or "honda" as the domains for the botnet and adware servers, explaining, "that lessens the suspicious activity . . . only dumbasses buy domains for there [sic] botnets and call it 1337-botnet.com."

206. On or about December 7, 2004, during a chat on AIM, ANCHETA explained to SoBe, "most ppl dont know that bnets how they spread all depends on what kind of bots your starting with, if you have a wide range of different isp bots you will spread a lot faster, thats why nets stop at a certain point its because theres nothing else to scan."

207. On or about December 7, 2004, during a chat on AIM, ANCHETA posted to SoBe a complaint message he had received from an internet hosting company that read "the IRC server controlling the bot drones is on port >6667, and the IRC channel is #syzt3m," commented to SoBe, "they forgot the # rofl so we are cool," told SoBe "I'm gonna msg them saying 'this irc network was investigated by my staff and we have removed the suspicious channel related to this'" and concluded, "haha always works."

208. On or about December 7, 2004, during a chat on AIM, ANCHETA told SoBe, "a tip to you is after setting up a bnet or irc or something illegal, do history -c, it will clear ur [your] history cmd's [commands]."

209. On or about December 7, 2004, ANCHETA received $1,306.52 from LOUDcash through Paypal.

//

210. On or about December 7, 2004, ANCHETA transferred $1,200 to SoBe through Paypal.

211. On or about December 7, 2004, ANCHETA discussed with SoBe over AIM the various advertising service companies for which they could serve as affiliates by using their botnets to install malicious code and make money, concluding "its immoral but the money makes it right."

212. On or about December 7, 2004, during a chat on AIM, ANCHETA and SoBe tested and modified the malicious code they were using to improve the efficiency and performance of the botnet and clickers.

213. On or about December 10, 2004, ANCHETA deposited a $2,732.96 check from Gammacash into his Wells Fargo Bank account.

214. On or about December 14, 2004, ANCHETA caused a computer on the computer network of the China Lake Naval Air Facility to attempt to connect to #syzt3m#, an IRC channel he controlled, located on an IRC server at Sago Networks leased by SoBe.

215. On or about December 20, 2004, ANCHETA transferred $149.00 from his Wells Fargo Bank account to FDCServers as payment for access to a server.

216. On or about December 24, 2004, ANCHETA deposited a $2,352.86 check from Gammacash into his Wells Fargo Bank account.

217. On or about January 5, 2005, ANCHETA caused a computer on the computer network of the China Lake Naval Air Facility to attempt to connect to #syzt3m#, an IRC channel he controlled, located on an IRC server at Sago Networks leased by SoBe.

218. On or about January 7, 2005, ANCHETA received $450.63 from LOUDcash through Paypal.

219. On or about January 8, 2005, ANCHETA transferred $425 to SoBe through Paypal.

220. On or about January 9, 2005, ANCHETA caused a computer on the computer network of the Defense Information Security Agency to attempt to connect to #syzt3m#, an IRC channel he controlled, located on an IRC server at Sago Networks leased be SoBe.

221. On or about January 10, 2005, ANCHETA deposited a $2,139.86 check from Gammacash into his Wells Fargo Bank account.

222. On or about January 21, 2005, ANCHETA deposited a $2,429.81 check from Gammacash into his Wells Fargo Bank account.

223. On or about February 6, 2005, ANCHETA caused a computer on the computer network of the Defense Information Security Agency to attempt to connect to #syzt3m#, an IRC channel he controlled, located on an IRC server at Sago Networks leased by SoBe.

224. On or about February 7, 2005, ANCHETA deposited a $2,988.11 check from Gammacash into his Wells Fargo Bank account.

225. On or about February 16, 2005, ANCHETA transferred $1,100 to SoBe through Paypal.

226. On or about February 16, 2005, ANCHETA caused the approximately 18,540 bots that had joined the IRC channel #syzt3m# to be redirected to navigate to an adware server located at FDCServers which he controlled, or to which he had access, and receive additional malicious code, namely, clickers.

227. On or about February 16, 2005, after FDCServers terminated ANCHETA's lease "for hosting malicious botnets," ANCHETA caused the topic in the IRC channel #syzt3m# to change to redirect the bots in that channel to navigate to a different adware server, one at EasyDedicated that he controlled, or to which he had access.

228. On or about February 17, 2005, ANCHETA caused the approximately 19,901 bots that had joined the IRC channel #syzt3m# to be redirected to navigate to an adware server located at EasyDedicated which he controlled, or to which he had access, and attempt to receive additional malicious code, namely, clickers.

229. On or about February 18, 2005, ANCHETA caused the approximately 21,973 bots that had joined the IRC channel #syzt3m# to be redirected to navigate to an adware server located at EasyDedicated which he controlled, or to which he had access, and attempt to receive additional malicious code, namely, clickers.

230. On or about February 22, 2005, ANCHETA or SoBe caused the approximately 19,148 bots that had joined the IRC channel #syzt3m# to be redirected to navigate to an adware server located at EasyDedicated which ANCHETA controlled, or to which ANCHETA had access, and attempt to receive additional malicious code, namely, clickers.

231. On or about February 24, 2005, ANCHETA or SoBe caused the approximately 23,410 bots that had joined the IRC channel #syzt3m# to be redirected to navigate to an adware server located at EasyDedicated which ANCHETA controlled, or to which ANCHETA had access, and attempt to receive additional malicious code, namely, clickers.

232. On or about February 25, 2005, ANCHETA or SoBe caused the approximately 19,205 bots that had joined the IRC channel #syzt3m# to be redirected to navigate to an adware server located at EasyDedicated which ANCHETA controlled, or to which ANCHETA had access, and attempt to receive additional malicious code, namely, clickers.

233. On or about February 25, 2005, ANCHETA deposited a $3,541.31 check from Gammacash into his Wells Fargo Bank account.

234. On or about February 27, 2005, ANCHETA caused the approximately 23,879 bots that had joined the IRC channel #syzt3m# to be redirected to navigate to an adware server located at EasyDedicated which ANCHETA controlled, or to which ANCHETA had access, and attempt to receive additional malicious code, namely, clickers.

235. On or about February 28, 2005, ANCHETA leased a server from Sago Networks.

236. On or about February 28, 2005, ANCHETA transferred $156.14 to Sago Networks through Paypal as payment for access to a server.

237. On or about February 28, 2005, ANCHETA caused the topic in the IRC channel #syzt3m# to change to redirect the approximately 27,494 bots that had joined the channel to navigate to a different adware server, namely to the one at Sago Networks he had just leased, and attempt to receive additional malicious code, namely, clickers.

238. On or about March 1, 2005, ANCHETA caused the approximately 23,879 bots that had joined the IRC channel #syzt3m# to be redirected to navigate to an adware server located at Sago Networks which he controlled, or to which he had access, and attempt to receive additional malicious code, namely, clickers.

239. On or about March 8, 2005, ANCHETA deposited a $3,188.21 check from Gammacash into his Wells Fargo Bank account.

240. On or about March 20, 2005, ANCHETA caused the approximately 17,957 bots that had joined the IRC channel #syzt3m#

to be redirected to navigate to an adware server located at Sago Networks which he controlled, or to which he had access, and attempt to receive additional malicious code, namely, clickers.

241. On or about March 22, 2005, ANCHETA deposited a $7,996.10 check from Gammacash into his Wells Fargo Bank account.

242. On or about March 23, 2005, ANCHETA caused the approximately 19,365 bots that had joined the IRC channel #syzt3m# to be redirected to navigate to an adware server located at Sago Networks which he controlled, or to which he had access, and attempt to receive additional malicious code, namely, clickers.

243. On or about April 3, 2005, ANCHETA transferred $185.50 to Sago Networks through Paypal as payment for access to a server.

244. On or about April 5, 2005, ANCHETA deposited a $6,336.86 check from Gammacash into his Wells Fargo Bank account.

245. On or about April 7, 2005, SoBe caused the approximately 14,244 bots that had joined the IRC channel #syzt3m# to be redirected to navigate to an adware server located at Sago Networks which ANCHETA controlled, or to which ANCHETA had access, and attempt to receive additional malicious code, namely, clickers.

246. On or about April 16, 2005, ANCHETA or SoBe caused the approximately 3,636 bots that had joined the IRC channel #syzt3m# to be redirected to navigate to an adware server located at Sago Networks which ANCHETA controlled, or to which ANCHETA had access, and attempt to receive additional malicious code, namely, clickers.

247. On or about April 22, 2005, ANCHETA deposited a $4,010.81 check from Gammacash into his Wells Fargo Bank account.

//

//

248. On or about April 27, 2005, ANCHETA or SoBe caused the approximately 7,779 bots that had joined the IRC channel #syzt3m# to be redirected to navigate to an adware server located at Sago Networks which ANCHETA controlled, or to which ANCHETA had access, and attempt to receive additional malicious code, namely, clickers.

249. On or about May 3, 2005, ANCHETA transferred $204.00 from his Wells Fargo Bank account to Sago Networks as payment for access to a server.

250. On or about May 20, 2005, ANCHETA deposited a $2,750.96 check from Gammacash into his Wells Fargo Bank account.

251. On or about June 9, 2005, ANCHETA deposited a $1,513.46 check from Gammacash into his Wells Fargo Bank account.

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

COUNT FIVE

[18 U.S.C. §§ 1030(a)(5)(A)(i), 1030(a)(5)(B)(v), and 1030(b)]

252. The Grand Jury hereby repeats and re-alleges all of the introductory allegations set forth in paragraphs 1 through 64, as well as paragraphs 98, 113, 114, 144 through 251 of this Indictment.

253. Beginning at least as early as December 13, 2004, and continuing through at least as late as January 26, 2005, in Los Angeles County, within the Central District of California, and elsewhere, defendant JEANSON JAMES ANCHETA knowingly caused the transmission of a program, information, code and command, and as a result of such conduct, intentionally caused damage without authorization to a protected computer used in interstate and foreign commerce and communication, namely, defendant JEANSON JAMES ANCHETA knowingly caused the transmission of malicious code to protected computers belonging to the China Lake Naval Air Facility that directed those computers to attempt to connect and connect to an IRC server outside the China Lake Naval Air Facility computer network to await further instructions, which, as a result of such conduct, caused damage affecting a computer system used by and for a government entity in furtherance of the administration of justice, national defense, and national security.

//

//

//

//

//

//

COUNT SIX

[18 U.S.C. §§ 1030(a)(5)(A)(i), 1030(a)(5)(B)(v), and 1030(b)]

254. The Grand Jury hereby repeats and re-alleges all of the introductory allegations set forth in paragraphs 1 through 64, as well as paragraphs 98, 113, 114, 144 through 251 of this Indictment.

255. Beginning at least as early as January 9, 2005, and continuing through at least as late as February 6, 2005, in Los Angeles County, within the Central District of California, and elsewhere, defendant JEANSON JAMES ANCHETA knowingly caused the transmission of a program, information, code and command, and as a result of such conduct, intentionally caused damage without authorization to a computer used in interstate and foreign commerce and communication, namely, defendant JEANSON JAMES ANCHETA knowingly caused the transmission of malicious code to protected computers belonging to the Defense Information Security Agency that directed those computers to attempt to connect and connect to an IRC server outside the Defense Information Security Agency computer network to await further instructions, which, as a result of such conduct, caused damage affecting a computer system used by and for a government entity in furtherance of the administration of justice, national defense, and national security.

//

//

//

//

//

//

COUNTS SEVEN THROUGH ELEVEN

[18 U.S.C. §§ 1030(a)(4) and 1030(b)]

256. The Grand Jury hereby repeats and re-alleges all of the introductory allegations set forth in paragraphs 1 through 64, as well as all of the allegations pertaining to the scheme to defraud set forth in paragraphs 98, 113, 114, 144 through 251 of this Indictment.

257. During on or about the following dates, in Los Angeles County, within the Central District of California, and elsewhere, defendant JEANSON JAMES ANCHETA knowingly and with intent to defraud accessed without authorization the following approximate numbers of computers involved in interstate and foreign commerce and communication, and furthered the intended fraud by installing adware on those computers without notice to or consent from the users of those computers, and by means of such conduct, obtained the following approximate monies from the following advertising service companies:

COUNT	APPROXIMATE DATES	APPROXIMATE NUMBER OF PROTECTED COMPUTERS ACCESSED WITHOUT AUTHORIZATION	APPROXIMATE PAYMENT
SEVEN	November 1, 2004 through November 19, 2004	26,975	$4,044.26 from Gammacash
EIGHT	November 16,2004 through December 7,2004	8,744	$1,306.52 from LOUDcash
NINE	January 15, 2005 through February 7, 2005	19,934	$2,988.11 from Gammacash

COUNT	APPROXIMATE DATES	APPROXIMATE NUMBER OF PROTECTED COMPUTERS ACCESSED WITHOUT AUTHORIZATION	APPROXIMATE PAYMENT
TEN	March 1, 2005 through March 22, 2005	53,321	$7,996.10 from Gammacash
ELEVEN	April 1, 2005 through April 22, 2005	28,066	$4,010.81 from Gammacash

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

COUNTS TWELVE THROUGH SIXTEEN

[18 U.S.C. § 1956(a)(1)(A)(i)]

258. The Grand Jury hereby repeats and re-alleges all of the introductory allegations set forth in paragraphs 1 through 64, as well as all of the allegations set forth in paragraphs 98, 113, 114, 144 through 258.

259. On or about the following dates, in Los Angeles County, within the Central District of California, and elsewhere, defendant JEANSON JAMES ANCHETA knowingly conducted the following financial transactions that involved the transfer of proceeds of specified unlawful activity, namely accessing protected computers to conduct fraud in violation of 18 U.S.C. §§ 1030(a)(4) and 1030(b), as alleged in Counts Seven through Eleven of this Indictment, which financial transactions affected interstate and foreign commerce, knowing that the property involved in each of the financial transactions represented the proceeds of some form, though not necessarily which form, of unlawful activity constituting a felony under federal, state, or foreign law, and with the intent to promote the carrying on of specified unlawful activity, namely, the transfer of payments to Internet hosting companies for access to the servers used to commit the intended fraud, as follows:

COUNT	APPROXIMATE DATE	APPROXIMATE AMOUNT	FINANCIAL TRANSACTION
TWELVE	November 23, 2004	$149.00	Transfer of funds from Wells Fargo Bank to FDCServers

COUNT	APPROXIMATE DATE	APPROXIMATE AMOUNT	FINANCIAL TRANSACTION
THIRTEEN	December 20, 2004	$149.00	Transfer of funds from Wells Fargo Bank to FDCServers
FOURTEEN	February 28, 2005	$157.14	Transfer of funds from Wells Fargo Bank to Sago Networks
FIFTEEN	April 3, 2005	$185.50	Transfer of funds from Wells Fargo Bank to Sago Networks
SIXTEEN	May 3, 2005	$204.00	Transfer of funds from Wells Fargo Bank to Sago Networks

//

//

//

//

//

//

//

//

//

//

//

//

//

//

COUNT SEVENTEEN

[18 U.S.C. § 982 and 21 U.S.C. § 853]

260. For the purpose of alleging forfeiture pursuant to Title 18, United States Code, Section 982, and Title 21, United States Code, Section 853, the Grand Jury hereby repeats and re-alleges each and every allegation of Counts One through Sixteen of this Indictment.

261. Pursuant to Title 18, United States Code, Section 982(a), defendant JEANSON JAMES ANCHETA, if convicted of one or more of the offenses alleged in Counts One through Sixteen, shall forfeit to the United States the following property:

a. All right, title, and interest in any and all property involved in each offense, or conspiracy to commit such offense, for which the defendant is convicted, and all property traceable to such property, including the following:

(1) the approximately $2,989.81 in proceeds generated from the sale of bots and proxies, as alleged in Counts One through Three of the Indictment, and deposited into Wells Fargo Bank accounts ending in the numbers 8032 and 7644 and linked to Paypal account resjames@sbcglobal.net;

(2) the approximately $58,357.86 in proceeds generated from the surreptitious install of adware on protected computers accessed without authorization, as alleged in Counts Four through Eleven of the Indictment, and deposited into a Wells Fargo Bank account ending in the numbers 8032 and 7644 and linked to Paypal account resjames@sbcglobal.net;

(3) a 1993 BMW 325is, Vehicle Identification Number WBABF4318PEK09502, California license plate number j4m3zzz, which

defendant JEANSON JAMES ANCHETA purchased on or about October 25, 2004 and improved thereafter with proceeds generated from the offenses alleged in Counts One through Eleven of the Indictment;

b. all money or other property that was the subject of each transaction, transportation, transmission or transfer in violation of Title 18, United States Code, Section 1956(a)(1)(A)(i), as alleged in Counts Twelve through Sixteen; and

c. all property used in any manner or part to commit or to facilitate the commission of those violations, including the following:

(1) one generic tower desktop computer containing a single internal hard disk, seized from the residence of defendant JEANSON JAMES ANCHETA on or about December 10, 2004;

(2) one IBM 2628 laptop computer, serial number 78-FFT63, seized from the residence of defendant JEANSON JAMES ANCHETA on or about December 10, 2004; and

(3) one Toshiba laptop computer, model number A7552212, serial number 35239783K seized from the residence of defendant JEANSON JAMES ANCHETA on or about May 26, 2005.

262. If, as a result of any act or omission by defendant JEANSON JAMES ANCHETA any of the foregoing money and property (a) cannot be located by the exercise of due diligence; (b) has been transferred, or sold to, or deposited with, a third party; (c) has been placed beyond the jurisdiction of the Court; (d) has been substantially diminished in value; or (e) has been commingled with other property that cannot be subdivided without difficulty, then any other property or interests of defendant

JEANSON JAMES ANCHETA, up to the value of the money and property described in the preceding paragraph of this Indictment, shall be subject to forfeiture to the United States.

A TRUE BILL

/S/

Foreperson

DEBRA WONG YANG
United States Attorney

THOMAS P. O'BRIEN
Assistant United States Attorney
Chief, Criminal Division

JAMES M. AQUILINA
Assistant United States Attorney
Cyber and Intellectual Property Crimes Section