

EXHIBIT 10.

1
2
3
4
5
6
7
8 UNITED STATES DISTRICT COURT
9 FOR THE CENTRAL DISTRICT OF CALIFORNIA
10 February 2005 Grand Jury

11 UNITED STATES OF AMERICA,) Case No. CR **DS-1060**
12)
13 Plaintiff,)
14) I N D I C T M E N T
15 v.)
16) [18 U.S.C. § 371: Conspiracy;
17 JEANSON JAMES ANCHETA,) 18 U.S.C. §§ 1030(a)(5)(A)(i),
18) (a)(5)(B)(i), and 1030(b): Attempted
19 Defendant.) Transmission of a Code, Information,
20) Program or Command to a Protected
21) Computer; 18 U.S.C. §§ 1030(a)(5)(A)(i)
22) and (a)(5)(B)(v): Transmission of
23) a Code, Information, Program or
24) Command to a Protected Computer
25) Used By a Government Entity;
26) 18 U.S.C. § 1030(a)(4): Accessing
27) Protected Computers to Conduct Fraud;
28) 18 U.S.C. § 1956(a)(1)(A)(i):
29) Promotional Money Laundering; 21 U.S.C.
30) § 853: Criminal Forfeiture]
31)

32 The Grand Jury charges:

33 **INTRODUCTORY ALLEGATIONS**

34 At all times relevant to this indictment:

35 DEFENDANT JEANSON JAMES ANCHETA

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

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

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

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

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

10 UNINDICTED CO-CONSPIRATOR IN BOCA RATON, FLORIDA

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

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

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

21 9. SoBe used the following user name: Serlissmc.

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

24 INTERNET SERVICE PROVIDERS

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

28 //

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

8 America Online

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

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

15 INTERNET HOSTING COMPANIES

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

25 EasyDedicated

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

28 //.

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

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

7 FDCServers

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

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

13 The Planet

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

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

19 Sago Networks

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

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

25 ADVERTISING SERVICE COMPANIES

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

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

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

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

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

22 Gammacash

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

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

1 | adware.

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

5 | LOUDcash

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

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

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

18 | PAYPAL

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

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

26 | CHINA LAKE NAVAL AIR FACILITY

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

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

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

5 DEFENSE INFORMATION SYSTEM AGENCY

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

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

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

16 NEXUS TO COMMERCE

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

20 COMPUTER TERMINOLOGY

21 Bot

22 44. The term "bot" is derived from the word "robot" and
23 commonly refers to a software program that performs repetitive
24 functions, such as indexing information on the Internet. Bots have
25 been created to perform tasks automatically on Internet Relay Chat
26 ("IRC") servers. The term "bot" also refers to computers that have
27 been infected with a program used to control or launch distributed
28 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

1 may become completely disabled and require significant repair.

2 Domain Name Server

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

13 Exe

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

20 Exploit

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

24 Internet Protocol Address

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

1 computer connected to the Internet must be assigned an IP address
2 so that Internet traffic sent from and directed to that computer
3 may be directed properly from its source to its destination. Most
4 ISPs control a range of IP addresses, which they assign to their
5 subscribers. No two computers on the Internet can have the same IP
6 address at the same time. Thus, at any given moment, an IP address
7 is unique to the computer to which it has been assigned.

8 Internet Relay Chat

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

19 Internet Relay Chat Daemon

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

23 Port

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

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

9 Root/Administrative Privileges

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

14 Server

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

28 //

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

1 infected user's computer.

2 Trojan

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

11 Uniform Resource Locator ("URL")

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

15 Worm

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

21 //

22 //

23 //

24 //

25 //

26 //

27 //

28 //

1 **COUNT ONE**

2 [18 U.S.C. § 371]

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

6 OBJECTS OF THE CONSPIRACY

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

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

20 b. To access without authorization a computer used in
21 interstate and foreign commerce and communication, and
22 intentionally initiate the transmission from and through that
23 computer of multiple commercial electronic mail messages that
24 affect interstate and foreign commerce, in violation of 18 U.S.C.
25 §§ 1037(a)(1), 1037(b)(2)(A), and 1037(b)(2)(F).

26 MEANS BY WHICH THE CONSPIRACY WAS TO BE ACCOMPLISHED

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

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

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

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

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

9 a. report to the IRC channel he controlled;

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

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

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

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

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

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

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

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

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

9 79. ANCHETA would accept payments through Paypal.

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

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

20 OVERT ACTS

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

26 Opening for Business

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

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

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

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

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

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

20 Sale to Circa

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

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

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

1 | Paypal totaling approximately \$400.

2 | Sale to KiD

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

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

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

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

17 | Sale to zxpl

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

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

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

1 zxpL had generated using his own botnet.

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

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

8 101. By on or about August 2, 2004, ANCHETA sold an exe and
9 1,500 bots to zxpL and received payment through Paypal, bringing
10 the number of bots available to zxpL for DDOS attacks to at least
11 8,500.

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

14 Improving the Business

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

21 Sales to Daytona and MLG

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

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

28 //

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

5 107. On or about August 9, 2004, ANCHETA sold an additional
6 400 bots to Daytona, and received payment through Paypal.

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

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

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

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

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

21 Sale to Teh1

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

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

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

4 115. Between on or about July 14, 2004 and on or about August
5 12, 2004, ANCHETA and Teh1 continued to negotiate the sale of the
6 exe.

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

9 Sale to Sploit

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

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

17 Sales to O_2iginal

18 119. On or about August 21, 2004, during a chat in IRC,
19 ANCHETA told an unindicted co-conspirator using the nickname
20 "o_2riginal" that he was hosting "around 100k bots total," that in
21 a week and a half 1,000 of his bots scanned and infected another
22 10,000, and that his botnet would be bigger if he had not used some
23 himself for "ddosing."

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

28 //

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

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

12 123. On or about August 21, 2004, ANCHETA sold o_2riginal
13 3,000 proxies, and received payment through Paypal.

14 124. On or about August 23, 2004, ANCHETA sold o_2riginal
15 2,000 bots and an exe that would cause the purchased bots to spread
16 or propagate, and received payment through Paypal.

17 125. From on or about August 23, 2004 through September 15,
18 2004, during chats in IRC, ANCHETA advised o_2riginal how to
19 maintain, update, and strengthen the purchased botnet.

20 Sale to Seminole Pride

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

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

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

4 Sale to Longwordus

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

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

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

14 Sale to a Confidential Source

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

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

24 134. On August 24, 2004, when the confidential source, posing
25 as a different user, contacted ANCHETA over AIM and asked "to buy
26 some bots for proxys," ANCHETA confirmed his ability to do so and
27 asked the confidential source to contact him "in a few hours."
28

1 135. On August 25, 2004, when the confidential source, posing
2 as yet another user, contacted ANCHETA over AIM and asked to
3 purchase a large botnet consisting of 20,000 compromised computers
4 with good attack power and the ability to send spam, ANCHETA told
5 the confidential source that he would be willing to sell only up to
6 2,000 bots.

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

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

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

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

27 //

28 //

1 140. On or about September 1, 2004, during a chat in IRC,
2 ANCHETA accessed his botnet and issued commands to rally or direct
3 2,000 bots to join the particular IRC channel ANCHETA had set up
4 for the confidential source.
5 //
6 //
7 //
8 //
9 //
10 //
11 //
12 //
13 //
14 //
15 //
16 //
17 //
18 //
19 //
20 //
21 //
22 //
23 //
24 //
25 //
26 //
27 //
28 //

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.

//

//

//

//

//

//

//

1 **COUNT FOUR**

2 [18 U.S.C. § 371]

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

6 OBJECTS OF THE CONSPIRACY

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

13 a. To knowingly cause the transmission of a program,
14 information, code and command, and as a result of such conduct,
15 intentionally cause damage without authorization to a computer
16 involved in interstate and foreign commerce and communication, and
17 cause loss aggregating more than \$5,000 in a one-year period, and
18 damage affecting a computer system used by and for a government
19 entity in furtherance of the administration of justice, national
20 defense, and national security, all in violation of 18 U.S.C.
21 §§ 1030(a)(5)(A)(i), 1030(a)(5)(B)(i), 1030(a)(5)(B)(v), and
22 1030(b); and

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

28 //

1 MEANS BY WHICH THE CONSPIRACY WAS TO BE ACCOMPLISHED

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

27 //

28 //

1 OVERT ACTS

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

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

9 163. On or about September 3, 2004, ANCHETA transferred
10 \$100.00 to Sago Networks through Paypal as payment for access to a
11 server.

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

18 165. On or about September 27, 2004, ANCHETA transferred
19 \$200.09 from his Wells Fargo Bank account to The Planet as payment
20 for access to a server.

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

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

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

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

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

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

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

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

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

1 ddos ==)." "

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

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

9 176. On or about October 20, 2004, ANCHETA deposited a
10 \$3,034.61 check from Gammacash into his Wells Fargo Bank account.

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

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

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

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

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

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

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

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

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

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

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

26 187. On or about November 5, 2004, ANCHETA deposited a
27 \$3,970.91 check from Gammacash into his Wells Fargo Bank account.

28 //

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

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

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

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

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

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

20 194. On or about November 19, 2004, ANCHETA deposited a
21 \$4,044.26 check from Gammacash into his Wells Fargo Bank account.

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

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

28 //

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

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

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

13 200. On or about November 23, 2004, ANCHETA transferred
14 \$149.00 from his Wells Fargo Bank account to FDCServers as payment
15 for access to a server.

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

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

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

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

1 and improve the "scanners."

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

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

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

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

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

28 //

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

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

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

12 213. On or about December 10, 2004, ANCHETA deposited a
13 \$2,732.96 check from Gammacash into his Wells Fargo Bank account.

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

18 215. On or about December 20, 2004, ANCHETA transferred
19 \$149.00 from his Wells Fargo Bank account to FDCServers as payment
20 for access to a server.

21 216. On or about December 24, 2004, ANCHETA deposited a
22 \$2,352.86 check from Gammacash into his Wells Fargo Bank account.

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

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

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

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

7 221. On or about January 10, 2005, ANCHETA deposited a
8 \$2,139.86 check from Gammacash into his Wells Fargo Bank account.

9 222. On or about January 21, 2005, ANCHETA deposited a
10 \$2,429.81 check from Gammacash into his Wells Fargo Bank account.

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

15 224. On or about February 7, 2005, ANCHETA deposited a
16 \$2,988.11 check from Gammacash into his Wells Fargo Bank account.

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

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

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

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

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

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

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

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

1 233. On or about February 25, 2005, ANCHETA deposited a
2 \$3,541.31 check from Gammacash into his Wells Fargo Bank account.

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

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

11 236. On or about February 28, 2005, ANCHETA transferred
12 \$156.14 to Sago Networks through Paypal as payment for access to a
13 server.

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

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

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

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

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

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

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

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

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

15 245. On or about April 7, 2005, SoBe caused the approximately
16 14,244 bots that had joined the IRC channel #syzt3m# to be
17 redirected to navigate to an adware server located at Sago Networks
18 which ANCHETA controlled, or to which ANCHETA had access, and
19 attempt to receive additional malicious code, namely, clickers.

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

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

27 //

28 //

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

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

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

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

13 //

14 //

15 //

16 //

17 //

18 //

19 //

20 //

21 //

22 //

23 //

24 //

25 //

26 //

27 //

28 //

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:

<u>COUNT</u>	<u>APPROXIMATE DATES</u>	<u>APPROXIMATE NUMBER OF PROTECTED COMPUTERS ACCESSED WITHOUT AUTHORIZATION</u>	<u>APPROXIMATE PAYMENT</u>
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

<u>COUNT</u>	<u>APPROXIMATE DATES</u>	<u>APPROXIMATE NUMBER OF PROTECTED COMPUTERS ACCESSED WITHOUT AUTHORIZATION</u>	<u>APPROXIMATE PAYMENT</u>
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:

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

<u>COUNT</u>	<u>APPROXIMATE DATE</u>	<u>APPROXIMATE AMOUNT</u>	<u>FINANCIAL TRANSACTION</u>
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

1 defendant JEANSON JAMES ANCHETA purchased on or about October 25,
2 2004 and improved thereafter with proceeds generated from the
3 offenses alleged in Counts One through Eleven of the Indictment;

4 b. all money or other property that was the subject of
5 each transaction, transportation, transmission or transfer in
6 violation of Title 18, United States Code, Section
7 1956(a)(1)(A)(i), as alleged in Counts Twelve through Sixteen;
8 and

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

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

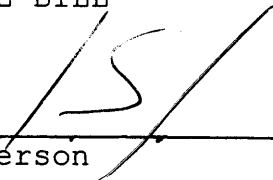
15 (2) one IBM 2628 laptop computer, serial number 78-
16 FFT63, seized from the residence of defendant JEANSON JAMES ANCHETA
17 on or about December 10, 2004; and

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

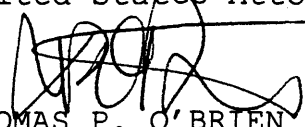
21 262. If, as a result of any act or omission by
22 defendant JEANSON JAMES ANCHETA any of the foregoing money and
23 property (a) cannot be located by the exercise of due diligence;
24 (b) has been transferred, or sold to, or deposited with, a third
25 party; (c) has been placed beyond the jurisdiction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

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

4
5 A TRUE BILL

6
7 
8 Foreperson

9 DEBRA WONG YANG
10 United States Attorney

11 
12 THOMAS P. O'BRIEN
13 Assistant United States Attorney
14 Chief, Criminal Division

15 JAMES M. AQUILINA
16 Assistant United States Attorney
17 Cyber and Intellectual Property Crimes Section
18
19
20
21
22
23
24
25
26
27
28

EXHIBIT 11.

P-SEND, ENTER, JS-3

**United States District Court
Central District of California**

UNITED STATES OF AMERICA vs.

Docket No. CR 05-1060-RGKDefendant JEANSON JAMES ANCHETASocial Security No. 8 6 8 3akas: Leon Ancheta; ResilienT

(Last 4 digits)

JUDGMENT AND PROBATION/COMMITMENT ORDER

In the presence of the attorney for the government, the defendant appeared in person on this date.

MONTH	DAY	YEAR
May	8	2006

COUNSEL**WITH COUNSEL**GREG WESLEY, DFPD

(Name of Counsel)

PLEA**GUILTY**, and the court being satisfied that there is a factual basis for the plea.**NOLO
CONTENDERE****NOT
GUILTY****FINDING**There being a finding/verdict of ☒ **GUILTY**, defendant has been convicted as charged of the offense(s) of:

Conspiracy in violation of 18 USC 371, as charged in Counts One and Four; Transmission of a Code, Information, Program or Command to a Protected Computer in violation of 18 USC 1030(a)(5)(A)(I) and (a)(5)(B)(v), as charged in Count Five; and Accessing Protected Computers to Commit Fraud in violation of 18 USC 1030(a)(4), as charged in Count Ten

**JUDGMENT
AND PROB/
COMM
ORDER**

The Court asked whether defendant had anything to say why judgment should not be pronounced. Because no sufficient cause to the contrary was shown, or appeared to the Court, the Court adjudged the defendant guilty as charged and convicted and ordered that:

It is ordered that the defendant shall pay to the United States a special assessment of \$400, which is due immediately.

The defendant shall comply with General Order 01-05.

Pursuant to U.S.S.G. Section 5E1.2(e) of the Guidelines, all fines are waived as it is found that the defendant does not have the ability to pay a fine.

It is ordered that the defendant shall pay restitution in the total amount of \$14,611.54 pursuant to 18 USC 3663A.

The amount of restitution ordered shall be paid as follows:

VictimAmount

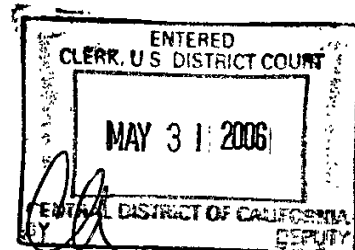
Defense Information System Agency \$4,337.94

Western Field Office

26722 Plaza Street, Suite 130

Mission Viejo, CA 92691

Attn: Robert Young, Defense Criminal Investigative Service, Computer Crimes Coordinator



35

2001

Amount

\$10,273.60

Pursuant to the Sentencing Reform Act of 1984, it is the judgment of the Court that the defendant, Jeanson Ancheta, is hereby committed on Counts One, Four, Five and Ten of the Indictment to the custody of the Bureau to be imprisoned for a term of FIFTY-SEVEN (57) months. This term consists of 57 months on each of Counts One, Four, Five, and Ten of the Indictment to be served concurrently.

1. The defendant shall comply with the rules and regulations of the U.S. Probation Office and General Order 318;
2. The defendant shall refrain from any unlawful use of a controlled substance. The defendant shall submit to one drug test within 15 days of release from imprisonment/placement on probation and at least two periodic drug tests thereafter, not to exceed eight tests per month, as directed by the Probation Officer;
3. During the period of community supervision the defendant shall pay the special assessment and restitution in accordance with this judgment's orders pertaining to such payment;
4. The defendant shall cooperate in the collection of a DNA sample from the defendant.
5. The defendant shall use only those computers and computer-related devices, screen user names, passwords, email accounts, and internet service providers (ISPs), as approved by the Probation Officer. Computers and computer-related devices include, but are not limited to, personal computers, personal data assistants (PDAs), internet appliances, electronic games, and cellular telephones, as well as their peripheral equipment, that can access, or can be modified to access, the internet, electronic bulletin boards, and other computers, or similar media;
6. All computers, computer-related devices, and their peripheral equipment, used by the defendant, shall be subject to search and seizure and the installation of search and/or monitoring software and/or hardware, including unannounced seizure for the purpose of search. The defendant shall not add, remove, upgrade, update, reinstall, repair, or otherwise modify the hardware or software on the computers, computer-related devices, or their peripheral equipment, nor shall he/she hide or encrypt files or data without prior approval of the Probation Officer. Further, the defendant shall provide all billing records, including telephone, cable, internet, satellite, and the like, as requested by the Probation Officer; and

USA vs. JEANSON JAMES ANCHETA

Docket No.: CR 05-1060-RGK

7. The defendant shall not possess or use a computer with access to any online service at any location (including his/her place of employment), without the prior approval of the Probation Officer. This includes access through any internet service provider, bulletin board system, or any public or private computer network system. The defendant shall not have another individual access the internet on his/her behalf to obtain files or information which he/she has been restricted from accessing himself/herself, or accept restricted files or information from another person.

All remaining counts are dismissed.

The Court recommends designation to a Bureau of Prisons facility in Southern California.

In addition to the special conditions of supervision imposed above, it is hereby ordered that the Standard Conditions of Probation and Supervised Release within this judgment be imposed. The Court may change the conditions of supervision, reduce or extend the period of supervision, and at any time during the supervision period or within the maximum period permitted by law, may issue a warrant and revoke supervision for a violation occurring during the supervision period.

MAY 26 2006

Date

R. Gary Klausner
R. GARY KLAUSNER, United States District Judge

It is ordered that the Clerk deliver a copy of this Judgment and Probation/Commitment Order to the U.S. Marshal or other qualified officer.

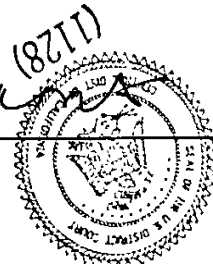
Sherri R. Carter, Clerk

MAY 26 2006

Filed Date

By A. Stillman

Deputy Clerk



USA vs. JEANSON JAMES ANCHETA

Docket No.: CR 05-1060-RGK

The defendant shall comply with the standard conditions that have been adopted by this court (set forth below).

STANDARD CONDITIONS OF PROBATION AND SUPERVISED RELEASE

While the defendant is on probation or supervised release pursuant to this judgment:

1. The defendant shall not commit another Federal, state or local crime;
2. the defendant shall not leave the judicial district without the written permission of the court or probation officer;
3. the defendant shall report to the probation officer as directed by the court or probation officer and shall submit a truthful and complete written report within the first five days of each month;
4. the defendant shall answer truthfully all inquiries by the probation officer and follow the instructions of the probation officer;
5. the defendant shall support his or her dependents and meet other family responsibilities;
6. the defendant shall work regularly at a lawful occupation unless excused by the probation officer for schooling, training, or other acceptable reasons;
7. the defendant shall notify the probation officer at least 10 days prior to any change in residence or employment;
8. the defendant shall refrain from excessive use of alcohol and shall not purchase, possess, use, distribute, or administer any narcotic or other controlled substance, or any paraphernalia related to such substances, except as prescribed by a physician;
9. the defendant shall not frequent places where controlled substances are illegally sold, used, distributed or administered;
10. the defendant shall not associate with any persons engaged in criminal activity, and shall not associate with any person convicted of a felony unless granted permission to do so by the probation officer;
11. the defendant shall permit a probation officer to visit him or her at any time at home or elsewhere and shall permit confiscation of any contraband observed in plain view by the probation officer;
12. the defendant shall notify the probation officer within 72 hours of being arrested or questioned by a law enforcement officer;
13. the defendant shall not enter into any agreement to act as an informer or a special agent of a law enforcement agency without the permission of the court;
14. as directed by the probation officer, the defendant shall notify third parties of risks that may be occasioned by the defendant's criminal record or personal history or characteristics, and shall permit the probation officer to make such notifications and to conform the defendant's compliance with such notification requirement;
15. the defendant shall, upon release from any period of custody, report to the probation officer within 72 hours;
16. and, for felony cases only: not possess a firearm, destructive device, or any other dangerous weapon.

- ☐ The defendant will also comply with the following special conditions pursuant to General Order 01-05 (set forth below).

STATUTORY PROVISIONS PERTAINING TO PAYMENT AND COLLECTION OF FINANCIAL SANCTIONS

The defendant shall pay interest on a fine or restitution of more than \$2,500, unless the court waives interest or unless the fine or restitution is paid in full before the fifteenth (15th) day after the date of the judgment pursuant to 18 U.S.C. §3612(f)(1). Payments may be subject to penalties for default and delinquency pursuant to 18 U.S.C. §3612(g). Interest and penalties pertaining to restitution, however, are not applicable for offenses completed prior to April 24, 1996.

If all or any portion of a fine or restitution ordered remains unpaid after the termination of supervision, the defendant shall pay the balance as directed by the United States Attorney's Office. 18 U.S.C. §3613.

The defendant shall notify the United States Attorney within thirty (30) days of any change in the defendant's mailing address or residence until all fines, restitution, costs, and special assessments are paid in full. 18 U.S.C. §3612(b)(1)(F).

The defendant shall notify the Court through the Probation Office, and notify the United States Attorney of any material change in the defendant's economic circumstances that might affect the defendant's ability to pay a fine or restitution, as required by 18 U.S.C. §3664(k). The Court may also accept such notification from the government or the victim, and may, on its own motion or that of a party or the victim, adjust the manner of payment of a fine or restitution-pursuant to 18 U.S.C. §3664(k). See also 18 U.S.C. §3572(d)(3) and for probation 18 U.S.C. §3563(a)(7).

Payments shall be applied in the following order:

1. Special assessments pursuant to 18 U.S.C. §3013;
2. Restitution, in this sequence:
 - Private victims (individual and corporate),
 - Providers of compensation to private victims,
 - The United States as victim;
3. Fine;
4. Community restitution, pursuant to 18 U.S.C. §3663(c); and
5. Other penalties and costs.

USA vs. JEANSON JAMES ANCHETADocket No.: CR 05-1060-RGK**SPECIAL CONDITIONS FOR PROBATION AND SUPERVISED RELEASE**

As directed by the Probation Officer, the defendant shall provide to the Probation Officer: (1) a signed release authorizing credit report inquiries; (2) federal and state income tax returns or a signed release authorizing their disclosure and (3) an accurate financial statement, with supporting documentation as to all assets, income and expenses of the defendant. In addition, the defendant shall not apply for any loan or open any line of credit without prior approval of the Probation Officer.

The defendant shall maintain one personal checking account. All of defendant's income, "monetary gains," or other pecuniary proceeds shall be deposited into this account, which shall be used for payment of all personal expenses. Records of all other bank accounts, including any business accounts, shall be disclosed to the Probation Officer upon request.

The defendant shall not transfer, sell, give away, or otherwise convey any asset with a fair market value in excess of \$500 without approval of the Probation Officer until all financial obligations imposed by the Court have been satisfied in full.

These conditions are in addition to any other conditions imposed by this judgment.

RETURN

I have executed the within Judgment and Commitment as follows:

Defendant delivered on _____ to _____
 Defendant noted on appeal on _____
 Defendant released on _____
 Mandate issued on _____
 Defendant's appeal determined on _____
 Defendant delivered on _____ to _____
 at _____

the institution designated by the Bureau of Prisons, with a certified copy of the within Judgment and Commitment.

United States Marshal

By _____

 Date

Deputy Marshal

CERTIFICATE: I hereby attest and certify this date that the foregoing document is a full, true and correct copy of the original on file in my office, and in my legal custody.

Clerk, U.S. District Court

By _____

 Filed Date

Deputy Clerk

USA vs. JEANSON JAMES ANCHETA Docket No.: CR 05-1060-RGK

FOR U.S. PROBATION OFFICE USE ONLY

Upon a finding of violation of probation or supervised release, I understand that the court may (1) revoke supervision, (2) extend the term of supervision, and/or (3) modify the conditions of supervision.

These conditions have been read to me. I fully understand the conditions and have been provided a copy of them.

(Signed) _____
Defendant Date _____

U. S. Probation Officer/Designated Witness Date _____

NOTICE PARTY SERVICE LIST

Case No. CR 05-1060-NGR Case Title USA v. ARCHETATitle of Document JUDGMENT AND COMMITMENT ORDER

	Atty Sttlmnt Officer Panel Coordinator
	BAP (Bankruptcy Appellate Panel)
	Beck, Michael J (Clerk, MDL Panel)
	BOP (Bureau of Prisons)
	CA St Pub Defender (Calif. State PD)
	CAAG (California Attorney General's Office - Keith H. Borjon, L.A. Death Penalty Coordinator)
	Case Asgmt Admin (Case Assignment Administrator)
	Catterson, Cathy (9 th Circuit Court of Appeal)
	Chief Deputy Admin
	Chief Deputy Ops
	Clerk of Court
	Death Penalty H/C (Law Clerks)
	Dep In Chg E Div
	Dep In Chg So Div
	Federal Public Defender
<input checked="" type="checkbox"/>	Fiscal Section ✓
	Intake Section, Criminal LA
	Intake Section, Criminal SA
	Intake Supervisor, Civil
	Interpreter Section
	PIA Clerk - Los Angeles (PIALA)
	PIA Clerk - Riverside (PIAED)
	PIA Clerk - Santa Ana (PIASA)
<input checked="" type="checkbox"/>	PSA - Los Angeles (PSALA) ✓
	PSA - Riverside (PSAED)
	PSA - Santa Ana (PSASA)
	Schnack, Randall (CJA Supervising Attorney)

	Statistics Clerk
	US Attorneys Office - Civil Division -L.A.
	US Attorneys Office - Civil Division - S.A.
	US Attorneys Office - Criminal Division -L.A.
	US Attorneys Office - Criminal Division -S.A.
	US Bankruptcy Court
<input checked="" type="checkbox"/>	US Marshal Service - Los Angeles (USMLA) ✓
	US Marshal Service - Riverside (USMED) ✓
	US Marshal Service -Santa Ana (USMSA)
<input checked="" type="checkbox"/>	US Probation Office (USPO) ✓
	US Trustee's Office
	Warden, San Quentin State Prison, CA

ADD NEW NOTICE PARTY (if sending by fax, mailing address must also be provided)	
Name:	
Firm:	
Address (include suite or floor):	
*E-mail:	
*Fax No.:	

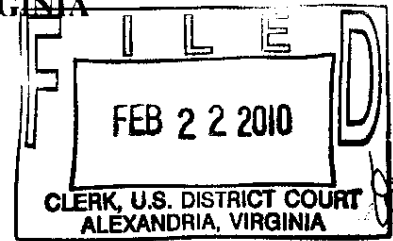
* For CIVIL cases only

JUDGE / MAGISTRATE JUDGE (list below):

Initials of Deputy Clerk slw

EXHIBIT 12.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division



MICROSOFT CORPORATION, a
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-27, CONTROLLING A
COMPUTER BOTNET THEREBY
INJURING MICROSOFT AND ITS
CUSTOMERS

Defendants.

Civil Action No: 1:10 cv 156 (LMB/JFA)

**EX PARTE TEMPORARY RESTRAINING ORDER AND
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

Plaintiff Microsoft Corp. ("Microsoft") has filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030), (2) the CAN-SPAM Act (15 U.S.C. § 7704), (3) the Electronic Communications Privacy Act (18 U.S.C. § 2701), (4) the Lanham Act (15 U.S.C. §§ 1125(a), (c)), and (5) the common law of trespass, unjust enrichment and conversion. Microsoft has moved *ex parte* for an emergency temporary restraining order and for an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure.

FINDINGS

The Court has considered the pleadings, declarations, exhibits, and memoranda filed in support of Microsoft's motion and finds that:

1. This Court has jurisdiction over the subject matter of this case and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon relief may be granted against the Defendants under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), CAN-

SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125) and the common law of trespass to chattels, unjust enrichment and conversion;

2. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125) and the common law of trespass to chattels, unjust enrichment and conversion, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. There is good cause to believe that, unless the Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125) and the common law of trespass to chattels, unjust enrichment and conversion. The evidence set forth in Microsoft's Brief in Support of Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Motion"), and the accompanying declarations and exhibits, demonstrates that Microsoft is likely to prevail on its claim that Defendants have engaged in violations of the foregoing laws by: intentionally accessing and sending malicious code to Microsoft's and its customers' protected computers and operating systems, without authorization, in order to infect those computers and make them part of the botnet, sending malicious code to configure, deploy and operate a botnet, sending unsolicited spam email to Microsoft's Hotmail accounts, sending unsolicited spam email that falsely indicate that they are from Microsoft's Hotmail accounts, collecting personal information including personal email addresses, and delivering malicious code including fake and misleading antivirus software. There is good cause to believe that such if such conduct continues, irreparable harm will occur to Microsoft, its customers and the public. There is good cause to believe that the Defendants

will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court;

4. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of the domains at issue in Microsoft's TRO Motion and other discoverable evidence of Defendants' misconduct available through such domains if the Defendants receive advance notice of this action. Based on the evidence cited in Microsoft's TRO Motion and accompanying declarations and exhibits, Microsoft is likely to be able to prove that: (1) the Defendants are engaged in activities that directly violate U.S. law and harms Microsoft, its customers and the public; (2) the Defendants have continued their unlawful conduct despite the clear injury to Microsoft, its customers and the public; (3) the Defendants are likely to relocate the domains at issue in Microsoft's TRO Motion and the harmful and malicious code disseminated through these domains and to warn its associates engaged in such activities if informed of Microsoft's action. Microsoft's request for this emergency *ex parte* relief is not the result of any lack of diligence on Microsoft's part, but instead is based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b) and Civil L.R. 65-1, good cause and the interests of justice require that this Order be Granted without prior notice to the Defendants, and, accordingly, Microsoft is relieved of the duty to provide the Defendants with prior notice of Microsoft's motion;

5. There is good cause to believe that the Defendants have engaged in illegal activity using .com Domains which are maintained by the top level domain registry Verisign, located in the United States and the Eastern District of Virginia.

6. There is good cause to believe that to immediately halt the injury caused by Defendants, Verisign must be ordered:

a. to immediately take all steps necessary to lock at the registry level the domains at

issue in the TRO Motion, and which are set forth at Appendix A hereto, to ensure that changes to the domain names cannot be made absent a court order;

- b. to immediately take all steps required to propagate to the foregoing domain registry changes to domain name registrars; and
- c. to hold the domains in escrow and take all steps necessary to ensure that the evidence of misconduct available through the domains be preserved.

7. There is good cause to permit notice of the instant order, notice of the Preliminary Injunction hearing and service of the Complaint by formal and alternative means, given the exigency of the circumstance and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, satisfy Fed. R. Civ. Pro. 4(f)(3) and are reasonably calculated to notify defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) personal delivery upon defendants who provided contact information in the U.S., (2) personal delivery through the Hague Convention on Service Abroad upon defendants who provided contact information in China, (3) transmission by e-mail, facsimile and mail to the contact information provided by defendants to their domain name registrars and as agreed to by defendants in their domain name registration agreements, (4) publishing notice on a publicly available Internet website.

TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

IT IS THEREFORE ORDERED that, Defendants and its representatives are temporarily restrained and enjoined from intentionally accessing and sending malicious code to Microsoft's and its customers' protected computers and operating systems, without authorization, in order to infect those computers and make them part of the botnet, sending malicious code to configure, deploy and operate a botnet, sending unsolicited spam email to Microsoft's Hotmail accounts, sending unsolicited spam email that falsely indicate that they are from Microsoft's Hotmail accounts, collecting personal information

including personal email addresses, and delivering malicious code including fake antivirus software, or undertaking any similar activity that inflicts harm on Microsoft, its customers or the public.

IT IS FURTHER ORDERED that, Defendants and its representatives are temporarily restrained and enjoined from configuring, deploying, operating or otherwise participating in or otherwise facilitating the botnet described in the TRO Motion, including but not limited to the domains at issue in the TRO motion and any other component or element of the botnet.

IT IS FURTHER ORDERED that Verisign must:

- a. immediately take all steps necessary to lock at the registry level the domains at issue in the TRO Motion, and which are set forth at Appendix A hereto, to ensure that changes to the domain names cannot be made absent a court order;
- b. immediately take all steps required to propagate to the foregoing domain registry changes to domain name registrars; and
- c. hold the domains in escrow and take all steps necessary to ensure that the evidence of misconduct available through the domains be preserved.

IT IS FURTHER ORDERED that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means authorized by law, including (1) by personal delivery upon defendants who provided contact information in the U.S., (2) personal delivery through the Hague Convention on Service Abroad upon defendants who provided contact information in China, (3) by transmission by e-mail, facsimile and mail to the contact information provided by defendants to their domain name registrars and as agreed to by defendants in their domain name registration agreements, (4) by publishing notice on a publicly available Internet website.

IT IS FURTHER ORDERED that the Temporary Restraining Order granted herein shall expire on March 8, 2010 at 9:00 a.m., unless within such time, the Order, for good cause shown, is extended for an additional period not to exceed fourteen (14) days, or unless it is further extended pursuant to Federal

Rule of Civil Procedure 65.

IT IS FURTHER ORDERED, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before this Court on March 8, 2010, at 9:00 a.m., to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against the Defendants, enjoining them from the conduct temporarily restrained by the preceding provisions of this order.

IT IS FURTHER ORDERED that the Defendants shall file with the Court and serve on Microsoft's counsel any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later than four (4) days prior to the hearing on Microsoft's request for a preliminary injunction. Microsoft may file responsive or supplemental pleadings, materials, affidavits, or memoranda with the Court and serve the same on counsel for the Defendants no later than one (1) day prior to the preliminary injunction hearing in this matter. Provided that service shall be performed by personal or overnight delivery, facsimile or electronic mail, and documents shall be delivered so that they shall be received by the other parties no later than 4:00 p.m. (Eastern Standard Time) on the appropriate dates listed in this paragraph.

IT IS FURTHER ORDERED that Microsoft shall maintain its bond in the amount of \$ \$54,600.⁰⁰, as payment of damages to which Defendants may be entitled for a wrongful injunction or restraint, during the pendency of this Action, or until further Order of the Court.

IT IS SO ORDERED

/s/ LMB
Leonie M. Brinkema
United States District Judge

Entered this 22ND day of February, 2010.

Appendix A

1. bestchristmascard.com
2. bestmirabella.com
3. bestyearcard.com
4. blackchristmascard.com
5. cardnewyear.com
6. cheapdecember.com
7. christmaslightsnow.com
8. decemberchristmas.com
9. directchristmasgift.com
10. eternalgreetingcard.com
11. freechristmassite.com
12. freechristmasworld.com
13. freedecember.com
14. funnychristmasguide.com
15. greatmirabellasite.com
16. greetingcardcalendar.com
17. greetingcardgarb.com
18. greetingguide.com
19. greetingsupersite.com
20. holidayxmas.com
21. itsfatherchristmas.com
22. justchristmasgift.com
23. lifegreetingcard.com
24. livechristmascard.com
25. livechristmasgift.com
26. mirabellaclub.com
27. mirabellamotors.com
28. mirabellanews.com
29. mirabellaonline.com
30. newlifeyearsite.com
31. newmediayearguide.com
32. newyearcardcompany.com
33. newyearcardfree.com
34. newyearcardonline.com
35. newyearcardservice.com
36. smartcardgreeting.com
37. superchristmasday.com
38. superchristmaslights.com
39. superyearcard.com
40. themirabelladirect.com
41. themirabellaguide.com
42. themirabellahome.com
43. topgreetingsite.com
44. whitewhitechristmas.com
45. worldgreetingcard.com
46. yourchristmaslights.com
47. yourdecember.com
48. yourmirabelladirect.com
49. yourregards.com
50. youryearcard.com
51. bestbarack.com
52. bestbaracksite.com
53. bestobamadirect.com
54. expowale.com
55. greatbarackguide.com
56. greatobamaguide.com
57. greatobamaonline.com
58. jobarack.com
59. superobamadirect.com
60. superobamaonline.com
61. thebaracksite.com
62. topwale.com
63. waledirekt.com
64. waleonline.com
65. waleprojekt.com
66. goodnewsdigital.com
67. goodnewsreview.com
68. linkworldnews.com
69. reportradio.com
70. spacemynews.com
71. wapcitynews.com
72. worldnewsdot.com
73. worldnewseye.com
74. worldtracknews.com
75. bestgoodnews.com
76. adorelyric.com
77. adorepoem.com
78. adoresongs.com

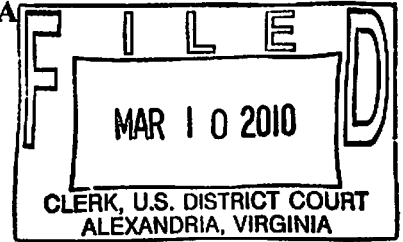
- | | |
|-------------------------------|--------------------------------|
| 79. bestadore.com | 120. greatsvallentine.com |
| 80. bestlovelong.com | 121. greatvallentinepoems.com |
| 81. funloveonline.com | 122. macride.com |
| 82. youradore.com | 123. mazdaautomotiveparts.com |
| 83. yourgreatlove.com | 124. mazdacarclub.com |
| 84. orldlovelife.com | 125. mazdaspeedzone.com |
| 85. romanticsloving.com | 126. netcitycab.com |
| 86. adoresong.com | 127. petcabtaxi.com |
| 87. bestlovehelp.com | 128. smartsalesgroup.com |
| 88. chatloveonline.com | 129. superpartycab.com |
| 89. cherishletter.com | 130. supersalesonline.com |
| 90. cherishpoems.com | 131. thecoupondiscount.com |
| 91. lovecentralonline.com | 132. themazdacar.com |
| 92. lovelifeportal.com | 133. themazdaspeed.com |
| 93. whocherish.com | 134. thevallentine lovers.com |
| 94. worldlovelife.com | 135. thevallentineparty.com |
| 95. worshiplove.com | 136. wirelessvallentineday.com |
| 96. yourteamdoc.com | 137. workcaredirect.com |
| 97. yourdatabank.com | 138. workhomegold.com |
| 98. alldatanow.com | 139. worklifedata.com |
| 99. alldataworld.com | 140. yourcountycoupon.com |
| 100. cantlosedata.com | 141. yourmazdacar.com |
| 101. freedoonline.com | 142. yourmazdatribute.com |
| 102. losenowfast.com | 143. yourvallentineday.com |
| 103. mingwater.com | 144. yourvallentinepoems.com |
| 104. theworldpool.com | 145. againstfear.com |
| 105. wagerpond.com | 146. antiterroralliance.com |
| 106. beadcareer.com | 147. antiterroris.com |
| 107. beadworkdirect.com | 148. antiterrornetwork.com |
| 108. bestcouponfree.com | 149. bayhousehotel.com |
| 109. bestmazdadealer.com | 150. bestblogdirect.com |
| 110. bluevallentineonline.com | 151. bestbreakingfree.com |
| 111. buymazdacars.com | 152. bestjournalguide.com |
| 112. codecouponsite.com | 153. bestlifeblog.com |
| 113. deathtaxi.com | 154. bestusablog.com |
| 114. funnyvallentinessite.com | 155. blogginhell.com |
| 115. greatcouponclub.com | 156. blogsitedirect.com |
| 116. greatmazdacars.com | 157. boarddiary.com |
| 117. greatsalesavailable.com | 158. breakingfreemichigan.com |
| 118. greatsalesgroup.com | 159. breakinggoodnews.com |
| 119. greatsalestax.com | 160. breakingkingnews.com |

161.	breakingnewsfm.com	202.	virtualesms.com
162.	breakingnewsfmltd.com	203.	wealthleaf.com
163.	debtbgonesite.com	204.	yourbarrier.com
164.	easyworldnews.com	205.	discountfreesms.com
165.	extendedman.com	206.	eccellentesms.com
166.	farboards.com	207.	freesmsorange.com
167.	fearalert.com	208.	ipersmstext.com
168.	globalantiterror.com	209.	morefreesms.com
169.	gonessite.com	210.	nuovosmsclub.com
170.	longballonline.com	211.	primosmsfree.com
171.	mobilephotoblog.com	212.	smsinlinea.com
172.	photoblogsite.com	213.	smsluogo.com
173.	residencehunter.com	214.	superioresms.com
174.	terroralertstatus.com	215.	4thfirework.com
175.	terrorfear.com	216.	biumer.com
176.	terrorismfree.com	217.	entrunk.com
177.	themostrateblog.com	218.	fireholiday.com
178.	tntbreakingnews.com	219.	fireworksholiday.com
179.	urbanfear.com	220.	fireworksnetwork.com
180.	usabreakingnews.com	221.	fireworkspoint.com
181.	yourbreakingnew.com	222.	freeindependence.com
182.	yourlength.com	223.	gemells.com
183.	yourlol.com	224.	handyphoneworld.com
184.	yourwent.com	225.	happyindependence.com
185.	bakeloaf.com	226.	holidayfirework.com
186.	chinamobilesms.com	227.	holidaysfirework.com
187.	coralarm.com	228.	holifireworks.com
188.	downloadfreesms.com	229.	interactiveindependence.com
189.	freecolorsms.com		
190.	freeservesms.com	230.	miosmschat.com
191.	fryroll.com	231.	movie4thjuly.com
192.	goldfixonline.com	232.	moviefireworks.com
193.	lastlabel.com	233.	movieindependence.com
194.	miosmsclub.com	234.	movies4thjuly.com
195.	moneymedal.com	235.	moviesfireworks.com
196.	nuovosms.com	236.	moviesindependence.com
197.	screenalias.com	237.	outdoorindependence.com
198.	smsclubnet.com	238.	smophi.com
199.	smsdiretto.com	239.	superhandycap.com
200.	smspianeta.com	240.	thehandygal.com
201.	tagdebt.com	241.	video4thjuly.com

- 242. videoindependence.com
- 243. yourhandyhome.com
- 244. yusitymp.com
- 245. aweleon.com
- 246. bedioger.com
- 247. bicodehl.com
- 248. birdab.com
- 249. cismosis.com
- 250. crucism.com
- 251. cycloro.com
- 252. encybest.com
- 253. favolu.com
- 254. framtr.com
- 255. frostep.com
- 256. gumentha.com
- 257. hindger.com
- 258. hornalfa.com
- 259. noloid.com
- 260. nonprobs.com
- 261. oughwa.com
- 262. painkee.com
- 263. pantali.com
- 264. pathoph.com
- 265. prerre.com
- 266. purgand.com
- 267. rascop.com
- 268. sodanthu.com
- 269. specipa.com
- 270. tabatti.com
- 271. tatumen.com
- 272. thingre.com
- 273. tobeyew.com

EXHIBIT 13.

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division**



MICROSOFT CORPORATION, a
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-27, CONTROLLING A
COMPUTER BOTNET THEREBY
INJURING MICROSOFT AND ITS
CUSTOMERS

Defendants.

Civil Action No: 1:10 CV 156 (LMB/JFA)

ORDER GRANTING PRELIMINARY INJUNCTION

Plaintiff Microsoft Corp. ("Microsoft") has filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030), (2) the CAN-SPAM Act (15 U.S.C. § 7704), (3) the Electronic Communications Privacy Act (18 U.S.C. § 2701), (4) the Lanham Act (15 U.S.C. §§ 1125(a), (c)), and (5) the common law of trespass, unjust enrichment and conversion. Microsoft has moved for a preliminary injunction pursuant to Rule 65 of the Federal Rules of Civil Procedure.

FINDINGS

The Court has considered the pleadings, declarations, exhibits, and memoranda filed in support of Microsoft's motion and finds that:

1. This Court has jurisdiction over the subject matter of this case and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against the Defendants under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications

Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125) and the common law of trespass to chattels, unjust enrichment and conversion;

2. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125) and the common law of trespass to chattels, unjust enrichment and conversion, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. There is good cause to believe that, unless the Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125) and the common law of trespass to chattels, unjust enrichment and conversion. The evidence set forth in Microsoft's Brief in Support of Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Motion"), and the accompanying declarations and exhibits, demonstrates that Microsoft is likely to prevail on its claim that Defendants have engaged in violations of the foregoing laws by: intentionally accessing and sending malicious code to Microsoft's and its customers' protected computers and operating systems, without authorization, in order to infect those computers and make them part of the botnet, sending malicious code to configure, deploy and operate a botnet, sending unsolicited spam email to Microsoft's Hotmail accounts, sending unsolicited spam email that falsely indicate that they are from Microsoft's Hotmail accounts, collecting personal information including personal email addresses, and delivering malicious code including fake

and misleading antivirus software. There is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft, its customers and the public. There is good cause to believe that the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court;

4. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of the domains at issue in Microsoft's TRO Motion and other discoverable evidence of Defendants' misconduct available through such domains if Defendants are not restrained by Order of this Court. Based on the evidence cited in Microsoft's TRO Motion and accompanying declarations and exhibits, Microsoft is likely to be able to prove that: (1) Defendants have operated through businesses and principals located outside of the United States; (2) the Defendants are engaged in activities that directly violate U.S. law and harms Microsoft, its customers and the public; (3) the Defendants have continued their unlawful conduct despite the clear injury to Microsoft, its customers and the public; (4) the Defendants are likely to relocate the domains at issue in Microsoft's TRO Motion and the harmful and malicious code disseminated through these domains if not restrained from doing so by Order of this Court. Therefore, in accordance with Fed. R. Civ. P. 65 and Civil L.R. 65-1, good cause and the interests of justice require that this Order be Granted;

5. There is good cause to believe that the Defendants, which are primarily individuals outside of the United States, have engaged in illegal activity using .com Domains which are maintained by the top level domain registry Verisign, located in the United States and the Eastern District of Virginia.

6. There is good cause to believe that to immediately prevent the injury caused by

Defendants, Verisign must be ordered:

- a. to immediately take all steps necessary to lock at the registry level the domains at issue in the TRO Motion and to remove all such domains from the zone file and to ensure that changes to the domain names cannot be made by Defendants absent a court order;
- b. to immediately take all steps required to propagate the foregoing domain registry changes to domain name registrars; and
- c. to hold the domains in escrow and take all steps necessary to ensure that the evidence of Defendants' misconduct available through the domains be preserved.

7. There is good cause to permit notice of the instant order and service of the Complaint by formal and alternative means, given the exigency of the circumstance and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, satisfy Fed. R. Civ. Pro. 4(f)(3) and are reasonably calculated to notify defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) personal delivery upon U.S. defendants, (2) personal delivery through the Hague Convention on Service Abroad upon Chinese defendants, (3) transmission by e-mail, facsimile and mail to the contact information provided by defendants to their domain name registrars and as agreed to by defendants in their domain name registration agreements, and (4) publication, including publishing notice on a publicly available Internet website.

PRELIMINARY INJUNCTION

IT IS THEREFORE ORDERED that, Defendants and its representatives are restrained and enjoined during the pendency of this action from intentionally accessing and sending

malicious code to Microsoft's and its customers' protected computers and operating systems, without authorization, in order to infect those computers and make them part of the botnet, sending malicious code to configure, deploy and operate a botnet, sending unsolicited spam email to Microsoft's Hotmail accounts, sending unsolicited spam email that falsely indicate that they are from Microsoft's Hotmail accounts, collecting personal information including personal email addresses, and delivering malicious code including fake antivirus software, or undertaking any similar activity that inflicts harm on Microsoft, its customers or the public.

IT IS FURTHER ORDERED that, Defendants and its representatives are restrained and enjoined during the pendency of this action from configuring, deploying, operating or otherwise participating in or otherwise facilitating the botnet described in the TRO Motion, including but not limited to the domains set forth at Appendix A hereto and any other component or element of the botnet.

IT IS FURTHER ORDERED that during the pendency of this action Verisign must:

- a. take all steps necessary to lock at the registry level the domains at issue in the TRO Motion and to remove all such domains from the zone file and to ensure that changes to the domain names cannot be made by Defendants absent a court order;
- b. take all steps required to propagate the foregoing domain registry changes to domain name registrars; and
- c. hold the domains in escrow and take all steps necessary to ensure that the evidence of misconduct available through the domains be preserved.

IT IS FURTHER ORDERED that copies of this Order and service of the Complaint may be carried out by any means authorized by law, including (1) by personal delivery upon

defendants who provided contact information in the U.S., (2) personal delivery through the Hague Convention on Service Abroad upon defendants who provided contact information in China, (3) by transmission by e-mail, facsimile and mail to the contact information provided by defendants to their domain name registrars and as agreed to by defendants in their domain name registration agreements, and (4) publication, including publishing notice on a publicly available Internet website.

IT IS FURTHER ORDERED that Microsoft shall maintain during the pendency of this action the bond it has posted in the amount of \$55,400, as payment of damages to which Defendants may be entitled for a wrongful injunction or restraint, during the pendency of this Action, or until further Order of the Court.

IT IS SO ORDERED

Entered this ^{ya}10 day of March, 2010.

ls/ LMB

Leonie M. Brinkema
United States District Judge

Appendix A

1. bestchristmascard.com
2. bestmirabella.com
3. bestyearcard.com
4. blackchristmascard.com
5. cardnewyear.com
6. cheapdecember.com
7. christmaslightsnow.com
8. decemberchristmas.com
9. directchristmasgift.com
10. eternalgreetingcard.com
11. freechristmassite.com
12. freechristmasworld.com
13. freedecember.com
14. funnychristmasguide.com
15. greatmirabellasite.com
16. greetingcardcalendar.com
17. greetingcardgarb.com
18. greetingguide.com
19. greetingsupersite.com
20. holidayxmas.com
21. itsfatherchristmas.com
22. justchristmasgift.com
23. lifegreetingcard.com
24. livechristmascard.com
25. livechristmasgift.com
26. mirabellaclub.com
27. mirabellamotors.com
28. mirabellaneews.com
29. mirabellaonline.com
30. newlifeyearsite.com
31. newmediayearguide.com
32. newyearcardcompany.com
33. newyearcardfree.com
34. newyearcardonline.com
35. newyearcardservice.com
36. smartcardgreeting.com
37. superchristmasday.com
38. superchristmaslights.com
39. superyearcard.com
40. themirabelladirect.com
41. themirabellaguide.com
42. themirabellahome.com
43. topgreetingsite.com
44. whitewhitechristmas.com
45. worldgreetingcard.com
46. yourchristmaslights.com
47. yourdecember.com
48. yourmirabelladirect.com
49. yourregards.com
50. youryearcard.com
51. bestbarack.com
52. bestbaracksite.com
53. bestobamadirect.com
54. expowale.com
55. greatbarackguide.com
56. greatobamaguide.com
57. greatobamaonline.com
58. jobarack.com
59. superobamadirect.com
60. superobamaonline.com
61. thebaracksite.com
62. topwale.com
63. waledirekt.com
64. waleonline.com
65. waleprojekt.com
66. goodnewsdigital.com
67. goodnewsreview.com
68. linkworldnews.com
69. reportradio.com
70. spacemynews.com
71. wapcitynews.com
72. worldnewsdot.com
73. worldnewseye.com
74. worldtracknews.com
75. bestgoodnews.com
76. adorelyric.com

- | | |
|------------------------------|-------------------------------|
| 77. adorepoem.com | 118. greatsalesgroup.com |
| 78. adoresongs.com | 119. greatsalestax.com |
| 79. bestadore.com | 120. greatsvallentine.com |
| 80. bestlovelong.com | 121. greatvalentinepoems.com |
| 81. funloveonline.com | 122. macride.com |
| 82. youradore.com | 123. mazdaautomotiveparts.com |
| 83. yourgreatlove.com | 124. mazdacarclub.com |
| 84. orldlovelife.com | 125. mazdaspeedzone.com |
| 85. romanticsloving.com | 126. netcitycab.com |
| 86. adoresong.com | 127. petcabtaxi.com |
| 87. bestlovehelp.com | 128. smartsalesgroup.com |
| 88. chatloveonline.com | 129. superpartycab.com |
| 89. cherishletter.com | 130. supersalesonline.com |
| 90. cherishpoems.com | 131. thecoupondiscount.com |
| 91. lovecentralonline.com | 132. themazdacar.com |
| 92. lovelifeportal.com | 133. themazdaspeed.com |
| 93. whocherish.com | 134. thevalentinelovers.com |
| 94. worldlovelife.com | 135. thevalentineparty.com |
| 95. worshiplove.com | 136. wirelessvalentineday.com |
| 96. yourteamdoc.com | 137. workcaredirect.com |
| 97. yourdatabank.com | 138. workhomegold.com |
| 98. alldatanow.com | 139. worklifedata.com |
| 99. alldataworld.com | 140. yourcountycoupon.com |
| 100. cantlosedata.com | 141. yourmazdacar.com |
| 101. freedoonline.com | 142. yourmazdatribute.com |
| 102. losenowfast.com | 143. yourvalentineday.com |
| 103. mingwater.com | 144. yourvalentinepoems.com |
| 104. theworldpool.com | 145. againstfear.com |
| 105. wagerpond.com | 146. antiterroralliance.com |
| 106. beadcareer.com | 147. antiterroris.com |
| 107. beadworkdirect.com | 148. antiterrornetwork.com |
| 108. bestcouponfree.com | 149. bayhousehotel.com |
| 109. bestmazdadealer.com | 150. bestblogdirect.com |
| 110. bluevalentineonline.com | 151. bestbreakingfree.com |
| 111. buymazdacars.com | 152. bestjournalguide.com |
| 112. codecouponsite.com | 153. bestlifeblog.com |
| 113. deathtaxi.com | 154. bestusablog.com |
| 114. funnyvalentinessite.com | 155. blogginhell.com |
| 115. greatcouponclub.com | 156. blogsitedirect.com |
| 116. greatmazdacars.com | 157. boarddiary.com |
| 117. greatsalesavailable.com | 158. breakingfreemichigan.com |

159.	breakinggoodnews.com	200.	smspaneta.com
160.	breakingkingnews.com	201.	tagdebt.com
161.	breakingnewsfm.com	202.	virtualesms.com
162.	breakingnewsltd.com	203.	wealthleaf.com
163.	debtbgonesite.com	204.	yourbarrier.com
164.	easyworldnews.com	205.	discountfreesms.com
165.	extendedman.com	206.	eccellentesms.com
166.	farboards.com	207.	freesmsorange.com
167.	fearalert.com	208.	ipersmstext.com
168.	globalantiterror.com	209.	morefreesms.com
169.	gonessite.com	210.	nuovosmsclub.com
170.	longballonline.com	211.	primosmsfree.com
171.	mobilephotoblog.com	212.	smsinlinea.com
172.	photoblogsite.com	213.	smsluogo.com
173.	residencehunter.com	214.	superioresms.com
174.	terroralertstatus.com	215.	4thfirework.com
175.	terrorfear.com	216.	blumer.com
176.	terrorismfree.com	217.	entrunk.com
177.	themostrateblog.com	218.	fireholiday.com
178.	tntbreakingnews.com	219.	fireworksholiday.com
179.	urbanfear.com	220.	fireworksnetwork.com
180.	usabreakingnews.com	221.	fireworkspoint.com
181.	yourbreakingnew.com	222.	freeindependence.com
182.	yourlength.com	223.	gemells.com
183.	yourlol.com	224.	handyphoneworld.com
184.	yourwent.com	225.	happyindependence.com
185.	bakeloaf.com	226.	holidayfirework.com
186.	chinamobilesms.com	227.	holidaysfirework.com
187.	coralarm.com	228.	holifireworks.com
188.	downloadfreesms.com	229.	interactiveindependence.com
189.	freecolorsms.com	230.	miosmschat.com
190.	freeservesms.com	231.	movie4thjuly.com
191.	fryroll.com	232.	moviefireworks.com
192.	goldfixonline.com	233.	movieindependence.com
193.	lastlabel.com	234.	movies4thjuly.com
194.	miosmsclub.com	235.	moviesfireworks.com
195.	moneymedal.com	236.	moviesindependence.com
196.	nuovosms.com	237.	outdoorindependence.com
197.	screenalias.com	238.	smphi.com
198.	smsclubnet.com	239.	superhandycap.com
199.	smsdiretto.com	240.	thehandygal.com

241. video4thjuly.com
242. videoindependence.com
243. yourhandyhome.com
244. yusitymp.com
245. aweleon.com
246. bedioger.com
247. bicodehl.com
248. blrdab.com
249. cismosis.com
250. crucism.com
251. cycloro.com
252. encybest.com
253. favolu.com
254. framtr.com
255. frostep.com
256. gumentha.com
257. hindger.com
258. hornalfa.com
259. noloid.com
260. nonprobs.com
261. oughwa.com
262. painkee.com
263. pantali.com
264. pathoph.com
265. prerre.com
266. purgand.com
267. rascop.com
268. sodanthu.com
269. specipa.com
270. tabatti.com
271. tatumen.com
272. thingre.com
273. tobeyew.com
274. broadwo.com
275. houreena.com
276. cyanian.com

EXHIBIT 14.

FILED
LODGED
ENTERED
RECEIVED
MAR - 9 2011
AT SEATTLE, COURT
CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
DEPUTY

The Honorable James L. Robart
CERTIFIED TRUE COPY
ATTEST: WILLIAM M. McCOOL
Clerk, U.S. District Court
Western District of Washington

By Mary Dutt
Deputy Clerk

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

MICROSOFT CORPORATION,

Plaintiff,

v.

JOHN DOES 1-11 CONTROLLING A
COMPUTER BOTNET THEREBY
INJURING MICROSOFT AND ITS
CUSTOMERS,

Defendants.

Case No. 2:11-cv-00222

**SECOND AMENDED [PROPOSED]
EX PARTE TEMPORARY
RESTRAINING ORDER, SEIZURE
ORDER AND ORDER TO SHOW
CAUSE RE PRELIMINARY
INJUNCTION**

****FILED UNDER SEAL****

Plaintiff Microsoft Corporation ("Microsoft") has filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) the CAN-SPAM Act (15 U.S.C. § 7704); (3) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); and (4) the common law of trespass, conversion and unjust enrichment. Microsoft has moved *ex parte* for an emergency temporary restraining order and seizure order pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C § 1116(d) (the Lanham Act) and 28 U.S.C. § 1651(a) (the All Writs Act), and an order to show cause why a preliminary injunction should not be granted.

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Microsoft's Application for *Ex Parte* Temporary Restraining Order, *Ex Parte* Seizure and Order

SECOND AMENDED [PROPOSED] EX PARTE
TEMPORARY RESTRAINING ORDER, SEIZURE
ORDER AND ORDER TO SHOW CAUSE RE
PRELIMINARY INJUNCTION

Orrick Herrington & Sutcliffe LLP
701 5th Avenue, Suite 5600
Seattle, Washington 98104-7097
tel+1-206-839-4300

1 to Show Cause Re Preliminary Injunction ("TRO Application"), the Court hereby makes the
2 following findings of fact and conclusions of law:

3 1. This Court has jurisdiction over the subject matter of this case and there is good
4 cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim
5 upon which relief may be granted against the Defendants under the Computer Fraud and Abuse
6 Act (18 U.S.C. § 1030); CAN-SPAM Act (15 U.S.C. § 7704); the Lanham Act (15 U.S.C. §§
7 1114, 1125); and the common law of trespass to chattels, conversion and unjust enrichment.

8 2. Microsoft owns the registered trademarks "Microsoft," "Windows," and "Hotmail"
9 used in connection with its services, software, and products.

10 3. There is good cause to believe that Defendants have engaged in and are likely to
11 engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030);
12 CAN-SPAM Act (15 U.S.C. § 7704); the Lanham Act (15 U.S.C. §§ 1114, 1125); and the
13 common law of trespass to chattels, conversion and unjust enrichment, and that Microsoft is,
14 therefore, likely to prevail on the merits of this action.

15 4. There is good cause to believe that, unless the Defendants are restrained and
16 enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants'
17 ongoing violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030); CAN-SPAM Act
18 (15 U.S.C. § 7704); the Lanham Act (15 U.S.C. §§ 1114, 1125); and the common law of trespass
19 to chattels, conversion and unjust enrichment. The evidence set forth in Microsoft's Application
20 for an Emergency Temporary Restraining Order, Seizure Order and Order to Show Cause Re
21 Preliminary Injunction ("TRO Motion"), and the accompanying declarations and exhibits,
22 demonstrates that Microsoft is likely to prevail on its claim that Defendants have engaged in
23 violations of the foregoing laws by: (1) intentionally accessing and sending malicious software to
24 Microsoft's and its customers' protected computers and operating systems, without authorization,
25 in order to infect those computers and make them part of the botnet; (2) sending malicious
26 software to configure, deploy and operate a botnet; (3) sending unsolicited spam e-mail to
27 Microsoft's Hotmail accounts; and (4) sending unsolicited spam e-mails that falsely indicate that
28 they are from or approved by Microsoft and that promote counterfeit pharmaceuticals and other

1 fraudulent schemes. There is good cause to believe that if such conduct continues, irreparable
2 harm will occur to Microsoft and the public, including Microsoft's customers. There is good
3 cause to believe that the Defendants will continue to engage in such unlawful actions if not
4 immediately restrained from doing so by Order of this Court.

5 5. There is good cause to believe that immediate and irreparable damage to this
6 Court's ability to grant effective final relief will result from the sale, transfer, or other disposition
7 or concealment by Defendants of the botnet command and control software that is hosted at and
8 otherwise operates through the Internet Protocol (IP) addresses listed in Appendix A and the
9 Internet domains at issue in Microsoft's TRO Application and from the destruction or
10 concealment of other discoverable evidence of Defendants' misconduct available at those
11 locations if the Defendants receive advance notice of this action. Based on the evidence cited in
12 Microsoft's TRO Application and accompanying declarations and exhibits, Microsoft is likely to
13 be able to prove that: (1) the Defendants are engaged in activities that directly violate U.S. law
14 and harm Microsoft and the public, including Microsoft's customers; (2) the Defendants have
15 continued their unlawful conduct despite the clear injury to the foregoing interests; (3) the
16 Defendants are likely to delete or relocate the botnet command and control software at issue in
17 Microsoft's TRO Application and the harmful, malicious, and trademark infringing software
18 disseminated through these IP addresses and domains and to warn their associates engaged in such
19 activities if informed of Microsoft's action. Microsoft's request for this emergency *ex parte* relief
20 is not the result of any lack of diligence on Microsoft's part, but instead is based upon the nature
21 of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b) and 15
22 U.S.C. § 1116(d), good cause and the interests of justice require that this Order be Granted
23 without prior notice to the Defendants, and accordingly Microsoft is relieved of the duty to
24 provide the Defendants with prior notice of Microsoft's motion.

25 6. There is good cause to believe that the Defendants have engaged in illegal activity
26 using the data centers and/or Internet hosting providers identified in Appendix A to host the
27 command and control software and the malicious botnet code and content used to maintain and
28 operate the botnet at computers, servers, electronic data storage devices or media at the IP

addresses identified in Appendix A.

7. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants' IP addresses identified in Appendix A must be immediately disabled; Defendants' computing resources related to such IP addresses must be disconnected from the Internet; Defendants must be prohibited from accessing Defendants' computer resources related to such IP addresses; and to prevent the destruction of data and evidence located on those computer resources.

8. There is good cause to believe that to immediately halt the injury caused by Defendants, and to ensure that future prosecution of this case is not rendered fruitless by attempts to delete, hide, conceal, or otherwise render inaccessible the software components that distribute unlicensed copies of Microsoft's registered trademarks and carry out other harmful conduct, with respect to Defendants' most current, active command and control IP addresses hosted at data centers operated by ECommerce, Inc.; FDCservers.net, LLC; Wholesale Internet, Inc.; Burstnet Technologies, Inc. d/b/a Network Operations Center, Inc.; and Softlayer Technologies, Inc., the United States Marshals Service in the judicial districts where the data centers are located should be directed to seize, impound and deliver into the custody of third-party escrow service Stroz Friedberg, 1925 Century Park East, Suite 1350, Los Angeles, CA 90067, all of Defendants' computers, servers, electronic data storage devices, software, data or media associated with the IP addresses listed in Appendix A.

9. There is good cause to believe that the Defendants have engaged in illegal activity using the Internet domains identified at Appendix B to this order to host the command and control software and content used to maintain and operate the botnet. There is good cause to believe that to immediately halt the injury caused by Defendants, each of Defendants' current and prospective domains set forth in Appendix B must be immediately made inaccessible, and/or removed from the Internet zone file.

10. There is good cause to direct that third party data centers, hosting providers and Internet registries/registrars reasonably assist in the implementation of the Order and refrain from frustrating the implementation and purposes of this Order, pursuant to 28 U.S.C. § 1651(a) (the

1 All Writs Act).

2 11. There is good cause to believe that if Defendants are provided advance notice of
3 Microsoft's TRO Application or this Order, they would move the botnet infrastructure, allowing
4 them to continue their misconduct and would destroy, move, hide, conceal, or otherwise make
5 inaccessible to the Court evidence of their misconduct, the botnet's activity, the infringing
6 materials, the instrumentalities used to make the infringing materials, and the records evidencing
7 the manufacture and distributing of the infringing materials.

8 12. There is good cause to permit notice of the instant order, notice of the Preliminary
9 Injunction hearing and service of the Complaint by formal and alternative means, given the
10 exigency of the circumstances and the need for prompt relief. The following means of service are
11 authorized by law, satisfy Due Process, satisfy Fed. R. Civ. Pro. 4(f)(3), and are reasonably
12 calculated to notify defendants of the instant order, the Preliminary Injunction hearing and of this
13 action: (1) personal delivery upon defendants who provided to the data centers and Internet
14 hosting providers contact information in the U.S.; (2) personal delivery through the Hague
15 Convention on Service Abroad or other treaties upon defendants who provided contact
16 information outside the United States; (3) transmission by e-mail, facsimile, and mail to the
17 contact information provided by defendants to the data centers, Internet hosting providers, and
18 domain registrars who host the software code associated with the IP addresses in Appendix A, or
19 through which domains in Appendix B are registered; and (4) publishing notice to the Defendants
20 on a publicly available Internet website.

21 13. There is good cause to believe that the harm to Microsoft of denying the relief
22 requested in its TRO Application outweighs any harm to any legitimate interests of Defendants
23 and that there is no undue burden to any third party.

24 **TEMPORARY RESTRAINING ORDER AND SEIZURE ORDER**

25 **IT IS THEREFORE ORDERED** as follows:

26 A. Defendants, their representatives and persons who are in active concert or
27 participation with them are temporarily restrained and enjoined from intentionally accessing and
28 sending malicious software to Microsoft's and its customers' protected computers and operating

1 systems, without authorization, in order to infect those computers and make them part of the
2 botnet; sending malicious software to configure, deploy and operate a botnet; sending unsolicited
3 spam e-mail to Microsoft's Hotmail accounts; and sending unsolicited spam e-mail that falsely
4 indicate that they are from or approved by Microsoft; or undertaking any similar activity that
5 inflicts harm on Microsoft or the public, including Microsoft's customers.

6 B. Defendants, their representatives and persons who are in active concert or
7 participation with them are temporarily restrained and enjoined from configuring, deploying,
8 operating or otherwise participating in or facilitating the botnet described in the TRO Application,
9 including but not limited to the command and control software hosted at and operating through the
10 IP addresses and domains set forth herein and through any other component or element of the
11 botnet in any location.

12 C. Defendants, their representatives and persons who are in active concert or
13 participation with them are temporarily restrained and enjoined from using the trademarks
14 "Microsoft," "Windows," "Hotmail," and/or other trademarks; trade names; service marks; or
15 Internet Domain addresses or names; or acting in any other manner which suggests in any way
16 that Defendants' products or services come from or are somehow sponsored or affiliated with
17 Microsoft, and from otherwise unfairly competing with Microsoft, misappropriating that which
18 rightfully belongs to Microsoft, or passing off their goods as Microsoft's.

19 D. Defendants, their representatives and persons who are in active concert or
20 participation with them are temporarily restrained and enjoined from infringing Microsoft's
21 registered trademarks, Registration Nos. 1200236, 2165601, 2463510 and others.

22 E. Defendants, their representatives and persons who are in active concert or
23 participation with them are temporarily restrained and enjoined from using in connection with
24 Defendants' activities any false or deceptive designation, representation or description of
25 Defendants' or of their representatives' activities, whether by symbols, words, designs or
26 statements, which would damage or injure Microsoft or give Defendants an unfair competitive
27 advantage or result in deception of consumers.

28 F. Defendants' materials bearing infringing marks, the means of making the

1 counterfeit marks, and records documenting the manufacture, sale, or receipt of things involved in
2 such violation, in the possession of data centers operated by ECommerce, Inc., FDCServers.net
3 LLC, Wholesale Internet, Inc., Burstnet Technologies, Inc., and Softlayer Technologies, Inc., all
4 pursuant to 15 U.S.C. §1116(d), shall be seized:

5 1. The seizure at the foregoing data centers and hosting providers shall take
6 place no later than seven (7) days after the date of issue of this order. The seizure may continue
7 from day to day, for a period not to exceed three (3) days, until all items have been seized. The
8 seizure shall be made by the United States Marshals Service. The United States Marshals Service
9 in the judicial districts where the foregoing data centers and hosting providers are located are
10 directed to coordinate with each other and with Microsoft and its attorneys in order to carry out
11 this Order such that disablement and seizure of the servers is effected simultaneously, to ensure
12 that Defendants are unable to operate the botnet during the pendency of this case. In order to
13 facilitate such coordination, the United States Marshals in the relevant jurisdictions are set forth,
14 as follows:

- 15
- 16 a. Northern District of Illinois
U.S. Marshal: Darryl K. McPherson
219 S. Dearborn Street, Room 2444
17 Chicago, IL 60604
(312) 353-5290
- 18
- 19 b. District of Colorado
U.S. Marshal: John Kammerzell
U.S. Courthouse
20 901 19th St., 3rd Floor
Denver, Co 80294
21 (303) 335-3400
- 22
- 23 c. Middle District of Pennsylvania
U.S. Marshal: Martin J. Pane (Acting)
Federal Building
24 Washington Avenue & Linden Street, Room 231
Scranton, PA 18501
25 (570) 346-7277
- 26
- 27 d. Western District of Missouri
U.S. Marshal: C. Mauri Sheer
U.S. Courthouse
28 400 E. 9th St., Room 3740
Kansas City, MO 64106
(816) 512-2000

- 1 e. Eastern District of Virginia
2 U.S. Marshal: John R. Hackman
3 401 Courthouse Square
4 Alexandria, VA 22314
5 (703) 837-5500
6
7 f. Northern District of Texas
8 U.S. Marshal: Randy Paul Ely
9 Federal Building
10 1100 Commerce Street, Room 16F47
11 Dallas, TX 75242
12 (214) 767-0836
13
14 g. Western District of Washington
15 U.S. Marshal: Mark L. Ericks
16 700 Stewart Street, Suite 9000
17 Seattle, WA 98101-1271
18 (206) 370-8600
19
20 h. Southern District of Ohio
21 U.S. Marshal: Cathy Jones
22 U.S. Courthouse
23 85 Marconi Boulevard, Room 460
24 Columbus, OH 43215
25 (614) 469-5540

2. The United States Marshals and their deputies shall be accompanied by Microsoft's attorneys and forensic experts at the foregoing described seizure, to assist with identifying, inventorying, taking possession of and isolating Defendants' computer resources, command and control software and other software components that are seized. The United States Marshals shall seize Defendants' computers, servers, electronic data storage devices or media associated with Defendants' IP addresses at the hosting companies set forth in Paragraph F above, or a live image of Defendants' data and information on said computers, servers, electronic data storage devices or media, as reasonably determined by the U.S. Marshals Service, Microsoft's forensic experts and/or attorneys.

3. Stroz Friedberg, 1925 Century Park East, Suite 1350, Los Angeles, CA 90067, tel. (310) 623-3301, will act as substitute custodian of any and all properties seized pursuant to this Order and shall hold harmless the United States Marshals Service, arising from any acts, incidents, or occurrences in connection with the seizure and possession of the defendants' property, including any third-party claims, and the United States Marshal shall be

1 discharged of his or her duties and responsibilities for safekeeping of the seized materials.

2 4. The United States Marshals accomplishing such seizure are permitted to
3 enter the premises of the data centers operated by ECommerce, Inc., FDCServers.net LLC,
4 Wholesale Internet, Inc., Burstnet Technologies, Inc., and Softlayer Technologies, Inc., in order to
5 serve copies of this Order, carry out the terms of this Order and to verify compliance with this
6 Order. The United States Marshals shall employ whatever reasonable means are necessary to
7 carry out the terms of this Order and to inspect the contents of any computers, servers, electronic
8 data storage devices, media, room, closets, cabinets, vehicles, containers or desks or documents
9 and to dismantle any equipment utilized by Defendants to carry out the activities prohibited by
10 this Order.

11 G. Pursuant to the All Writs Act and to effect discovery of the true identities of the
12 John Doe defendants, the data centers and hosting providers identified in Appendix A and the
13 domain registries identified in Appendix B to this Order, shall:

14 1. disable Defendants' IP addresses set forth in Appendix A (including
15 through any backup systems) so that they can no longer be accessed over the Internet, connected
16 to, or communicated with in any way except as explicitly provided for in this order;

17 2. disable Defendants' domains set forth in Appendix B so that they can no
18 longer be accessed over the Internet, connected to, or communicated with in any way except as
19 explicitly provided for in this order by (1) locking the domains and removing such domains from
20 the zone file and (2) taking all steps required to propagate the foregoing domain registry changes
21 to domain name registrars;

22 3. transfer any content and software hosted on Defendants' IP addresses listed
23 in Appendix A to new IP addresses not listed in Appendix A; notify Defendants and any other
24 owners of such content or software of the new IP addresses, and direct them to contact
25 Microsoft's Counsel, Gabriel M. Ramsey, Orrick Herrington & Sutcliffe, 1000 Marsh Road,
26 Menlo Park, CA 90425-1015, (Tel: 650-614-7400), to facilitate any follow-on action;

27 4. preserve and produce to Microsoft documents and information sufficient to
28 identify and contact Defendants and Defendants' representatives operating or controlling the IP

1 addresses set forth in Appendix A, including any and all individual or entity names, mailing
2 addresses, e-mail addresses, facsimile numbers and telephone numbers or similar contact
3 information, including but not limited to such contact information reflected in billing, usage and
4 contact records;

5 5. provide reasonable assistance in implementing the terms of this Order and
6 shall take no action to frustrate the implementation of this Order, including the provision of
7 sufficient and reasonable access to offices, facilities, computer networks, computers and services,
8 so that the United States Marshals Service, Microsoft, its attorneys and/or representatives may
9 directly supervise and confirm the implementation of this Order against Defendants;

10 6. refrain from publishing or providing notice or warning of this Order to
11 Defendants, their representatives or persons who are in active concert or participation with them,
12 until this Order is fully executed, except as explicitly provided for in this Order.

13 H. Anyone interfering with the execution of this Order is subject to arrest by federal or
14 state law enforcement officials.

15 **IT IS FURTHER ORDERED** that copies of this Order, notice of the Preliminary
16 Injunction hearing and service of the Complaint may be served by any means authorized by law,
17 including (1) by personal delivery upon defendants who provided contact information in the U.S.;
18 (2) personal delivery through the Hague Convention on Service Abroad upon defendants who
19 provided contact information outside the U.S.; (3) by transmission by e-mail, facsimile and mail
20 to the contact information provided by defendants to the data centers, Internet hosting providers
21 and domain registrars who hosted the software code associated with the IP addresses set forth at
22 Appendix A or through which domains in Appendix B are registered; and (4) by publishing notice
23 to Defendants on a publicly available Internet website.

24 **IT IS FURTHER ORDERED**, pursuant to Federal Rule of Civil Procedure 65(b), 15
25 U.S.C. §1116(d)(10) and 28 U.S.C. § 1651(a) (the All Writs Act) that the Defendants shall appear
26 before this Court within 28 days from the date of this order, to show cause, if there is any, why
27 this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against
28 the Defendants, enjoining them from the conduct temporarily restrained by the preceding

1 provisions of this Order.

2 **IT IS FURTHER ORDERED** that Microsoft shall post bond in the amount of \$173,000
3 as cash to be paid into the Court registry.

4 **IT IS FURTHER ORDERED** that Microsoft shall compensate the data centers, Internet
5 hosting providers and/or domain registries identified in Appendices A and B at prevailing rates for
6 technical assistance rendered in implementing the Order.

7 **IT IS FURTHER ORDERED** that this Order shall be implemented with the least degree
8 of interference with the normal operation of the data centers and internet hosting providers and/or
9 domain registries identified in Appendices A and B consistent with thorough and prompt
10 implementation of this Order. *All actions undertaken under the authority of this
Order shall be in strict compliance with 15 U.S.C. § 1116.*

11 **IT IS FURTHER ORDERED** that the Defendants shall file with the Court and serve on
12 Microsoft's counsel any answering affidavits, pleadings, motions, expert reports or declarations
13 and/or legal memoranda no later than four (4) days prior to the hearing on Microsoft's request for
14 a preliminary injunction. Microsoft may file responsive or supplemental pleadings, materials,
15 affidavits, or memoranda with the Court and serve the same on counsel for the Defendants no later
16 than one (1) day prior to the preliminary injunction hearing in this matter. Provided that service
17 shall be performed by personal or overnight delivery, facsimile or electronic mail, and documents
18 shall be delivered so that they shall be received by the other parties no later than 4:00 p.m. (Pacific
19 Standard Time) on the appropriate dates listed in this paragraph.

20 **IT IS SO ORDERED**

21
22 Entered this 9th day of March, 2011.
23 at 9:00am.

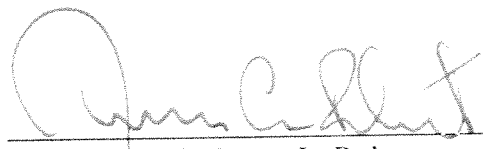
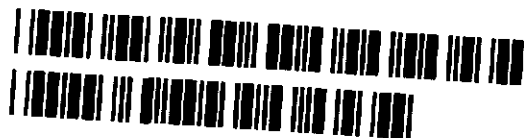

The Honorable James L. Robart
United States District Judge

EXHIBIT 15.

FILED
LODGED
APR - 6 2011
AT SEATTLE
CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
DEPUTY

The Honorable James L. Robart



11-CV-00222-ORD

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

MICROSOFT CORPORATION,

Plaintiff,

v.

JOHN DOES 1-11 CONTROLLING A
COMPUTER BOTNET THEREBY
INJURING MICROSOFT AND ITS
CUSTOMERS,

Defendants.

Case No. 2:11-cv-00222

~~PROPOSED~~ ORDER FOR
PRELIMINARY INJUNCTION

Plaintiff Microsoft Corporation ("Microsoft") filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) the CAN-SPAM Act (15 U.S.C. § 7704); (3) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); and (4) the common law of trespass, conversion and unjust enrichment. On March 9, 2011, the Court granted Microsoft's Application for an Emergency Temporary Restraining Order, Seizure Order and Order to Show Cause Re Preliminary Injunction. Microsoft now moves for an Order for Preliminary Injunction seeking to keep in place the relief granted by the March 9th order.

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Microsoft's Application for *Ex Parte* Temporary Restraining Order, *Ex Parte* Seizure and Order to Show Cause Re Preliminary Injunction ("TRO Application"), as well as supplemental

1 declarations and a status report regarding notice and service of process submitted by Microsoft
2 on April 4, 2011, the Court hereby makes the following findings of fact and conclusions of law:

3 1. This Court has jurisdiction over the subject matter of this case and there is good
4 cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim
5 upon which relief may be granted against the Defendants under the Computer Fraud and Abuse
6 Act (18 U.S.C. § 1030); CAN-SPAM Act (15 U.S.C. § 7704); the Lanham Act (15 U.S.C. §§
7 1114, 1125); and the common law of trespass to chattels, conversion and unjust enrichment.

8 2. Microsoft owns the registered trademarks "Microsoft," "Windows," and
9 "Hotmail," used in connection with its services, software, and products.

10 3. There is good cause to believe that Defendants have engaged in and are likely to
11 engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030);
12 CAN-SPAM Act (15 U.S.C. § 7704); the Lanham Act (15 U.S.C. §§ 1114, 1125); and the
13 common law of trespass to chattels, conversion and unjust enrichment. The evidence set forth in
14 Microsoft's Application for an Emergency Temporary Restraining Order, Seizure Order and
15 Order to Show Cause Re Preliminary Injunction ("TRO Motion"), and the accompanying
16 declarations and exhibits, demonstrates that Microsoft is likely to prevail on its claim that
17 Defendants have engaged in violations of the foregoing laws by: (1) intentionally accessing and
18 sending malicious software to Microsoft's and its customers' protected computers and operating
19 systems, without authorization, in order to infect those computers and make them part of the
20 botnet; (2) sending malicious software to configure, deploy and operate a botnet; (3) sending
21 unsolicited spam e-mail to Microsoft's Hotmail accounts; and (4) sending unsolicited spam e-
22 mails that falsely indicate that they are from or approved by Microsoft and that promote
23 counterfeit pharmaceuticals and other fraudulent schemes. Therefore, Microsoft is likely to
24 prevail on the merits of this action.

25 4. There is good cause to believe that unless they are preliminarily enjoined by
26 Order of this Court, immediate and irreparable harm will result from the Defendants' further
27 violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030); CAN-SPAM Act (15
28 U.S.C. § 7704); the Lanham Act (15 U.S.C. §§ 1114, 1125); and the common law of trespass to

1 chattels, conversion and unjust enrichment. There is good cause to believe that if such conduct
2 continues, irreparable harm will occur to Microsoft and the public, including Microsoft's
3 customers. There is good cause to believe that the Defendants will continue to engage in such
4 unlawful actions if not preliminarily enjoined from doing so by Order of this Court.

5 5. There is good cause to believe that the hardship to Microsoft, its customers, and
6 the public resulting from denying this Motion for Preliminary Injunction far outweighs the
7 hardship that will be suffered by Defendants if the Preliminary Injunction issues. Defendants are
8 accused of illegally infecting end-user computers to enlist them into Rustock, a network of
9 infected end-user computers operated over the Internet and used for illegal purposes. Microsoft,
10 its customers, and the public are harmed by this activity through the high-volume of spam e-mail
11 generated by Rustock, the various schemes promoted by Rustock e-mail such as the sale of
12 counterfeit pharmaceuticals, and the ongoing infection of end-user computers and their use in
13 illegal purposes. Therefore, the balance of hardships tips in favor of granting a Preliminary
14 Injunction.

15 6. There is good cause to believe that the preliminary injunction will benefit the
16 public. Maintaining the relief put in place under the Court's TRO will keep the operators of
17 Rustock from reconstituting its Command and Control Infrastructure, will sharply curtail its
18 ability to propagate spam e-mail, will reduce its involvement in promoting illegal schemes
19 including infringement of Microsoft's trademarks and the sale of counterfeit pharmaceuticals,
20 and will keep it from using the current tier of Rustock-infected end-user computers in illegal
21 activity without their owner's permission or knowledge. Therefore, a Preliminary Injunction will
22 have a favorable impact on the public interest.

23 7. There is good cause to believe that the Defendants have engaged in illegal activity
24 using the data centers and/or Internet hosting providers identified in Appendix A to host the
25 command and control software and the malicious botnet code and content used to maintain and
26 operate the botnet at computers, servers, electronic data storage devices or media at the IP
27 addresses identified in Appendix A.

28 8. There is good cause to believe that to keep Defendants from resuming actions

1 injurious to Microsoft and others, Defendants' IP addresses identified in Appendix A must
2 remain in a disabled state; Defendants' computing resources related to such IP addresses must
3 remain disconnected from the Internet; and Defendants must be prohibited from accessing
4 Defendants' computer resources related to such IP addresses.

5 9. There is good cause to believe that the Defendants have engaged in illegal activity
6 using the Internet domains identified at Appendix B to this order to host the command and
7 control software and content used to maintain and operate the botnet. There is good cause to
8 believe that to immediately halt the injury caused by Defendants, each of Defendants' current
9 and prospective domains set forth in Appendix B must be maintained in an inaccessible state,
10 and/or removed from the Internet zone file.

11 10. There is good cause to direct that third party data centers, hosting providers and
12 Internet registries/registrars reasonably assist in the implementation of the Order and refrain from
13 frustrating the implementation and purposes of this Order, pursuant to 28 U.S.C. § 1651(a) (the
14 All Writs Act).

15 11. There is good cause to believe that Microsoft has provided adequate notice to
16 Defendants of the TRO and this Preliminary Injunction. The following means of service
17 employed by Microsoft are authorized by law, satisfy Due Process, satisfy Fed. R. Civ. Pro.
18 4(f)(3); and are reasonably calculated to notify defendants of the TRO, the Preliminary
19 Injunction hearing and of the Complaint: (1) transmission by e-mail, facsimile, and mail to the
20 contact information provided by defendants to the data centers, Internet hosting providers, and
21 domain registrars who host the software code associated with the IP addresses in Appendix A, or
22 through which domains in Appendix B are registered; and (2) publishing notice to the
23 Defendants on a publicly available Internet website.

24 12. Therefore, in accordance with Fed. R. Civ. P. 65(a) and the All Writs Act, good
25 cause and the interests of justice require that this Order be Granted.

26 **PRELIMINARY INJUNCTION**

27 **IT IS THEREFORE ORDERED** as follows:

28 A. Defendants, their representatives and persons who are in active concert or

1 participation with them are preliminarily enjoined from intentionally accessing and sending
2 malicious software to Microsoft's and its customers' protected computers and operating systems,
3 without authorization, in order to infect those computers and make them part of the botnet;
4 sending malicious software to configure, deploy and operate a botnet; sending unsolicited spam
5 e-mail to Microsoft's Hotmail accounts; and sending unsolicited spam e-mail that falsely indicate
6 that they are from or approved by Microsoft; or undertaking any similar activity that inflicts
7 harm on Microsoft or the public, including Microsoft's customers.

8 B. Defendants, their representatives and persons who are in active concert or
9 participation with them are preliminarily enjoined from configuring, deploying, operating or
10 otherwise participating in or facilitating the botnet described in the TRO Application, including
11 but not limited to the command and control software hosted at and operating through the IP
12 addresses and domains set forth herein and through any other component or element of the
13 botnet in any location.

14 C. Defendants, their representatives and persons who are in active concert or
15 participation with them are preliminarily enjoined from using the trademarks "Microsoft,"
16 "Windows," "Hotmail," and/or other trademarks; trade names; service marks; or Internet Domain
17 addresses or names; or acting in any other manner which suggests in any way that Defendants'
18 products or services come from or are somehow sponsored or affiliated with Microsoft, and from
19 otherwise unfairly competing with Microsoft, misappropriating that which rightfully belongs to
20 Microsoft, or passing off their goods as Microsoft's.

21 D. Defendants, their representatives and persons who are in active concert or
22 participation with them are preliminarily enjoined from infringing Microsoft's registered
23 trademarks, Registration Nos. 1200236, 2165601, 2463510 and others.

24 E. Defendants, their representatives and persons who are in active concert or
25 participation with them are preliminarily enjoined from using in connection with Defendants'
26 activities any false or deceptive designation, representation or description of Defendants' or of
27 their representatives' activities, whether by symbols, words, designs or statements, which would
28 damage or injure Microsoft or give Defendants an unfair competitive advantage or result in

1 deception of consumers.

2 F. Microsoft shall maintain its bond in the amount of \$173,000 that it has paid into
3 the Court's Registry.

4 G. Pursuant to the All Writs Act, the data centers and hosting providers identified in
5 Appendix A and the domain registries identified in Appendix B to this Order, shall, during the
6 pendency of this action:

7 1. Maintain in a disabled state Defendants' IP addresses set forth in
8 Appendix A (including through any backup systems) so that they cannot be accessed over the
9 Internet, connected to, or communicated with in any way except as explicitly provided for in this
10 order;

11 2. Maintain in a disabled state Defendants' domains set forth in Appendix B
12 so that they cannot be accessed over the Internet, connected to, or communicated with in any
13 way except as explicitly provided for in this order by (1) keeping the domains locked and
14 keeping such domains from being entered into the zone file; and (2) taking all steps required to
15 propagate the foregoing domain registry changes to domain name registrars;

16 3. provide reasonable assistance in implementing the terms of this Order and
17 shall take no action to frustrate the implementation of this Order.

18
19
20 **IT IS SO ORDERED**

21 Entered this th 6 day of April, 2011.

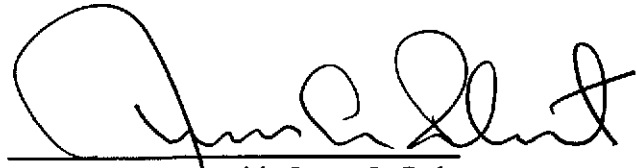
22 
23 The Honorable James L. Robart
24 United States District Judge
25
26
27
28

EXHIBIT 16.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division



MICROSOFT CORPORATION, a
Washington corporation,

Plaintiff,

v.

DOMINIQUE ALEXANDER PATTI, an
individual; DOTFREE GROUP S.R.O., a
Czech limited liability company, JOHN
DOES 1-22, CONTROLLING A
COMPUTER BOTNET THEREBY
INJURING MICROSOFT AND ITS
CUSTOMERS

Defendants.

Civil Action No: 1:11cv1017

FILED UNDER SEAL

**EX PARTE TEMPORARY RESTRAINING ORDER AND
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

Plaintiff Microsoft Corp. ("Microsoft") has file a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) the CAN-SPAM Act (15 U.S.C. § 7704); (3) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); and (4) the common law of trespass, unjust enrichment, conversion, and negligence. Microsoft has moved *ex parte* for an emergency temporary restraining order and an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure and the All-Writs Act, 28 U.S.C. § 1651.

FINDINGS

The Court has considered the pleadings, declarations, exhibits, and memorandum filed in support of Microsoft's motion and finds that:

1. This Court has jurisdiction over the subject matter of this case and there is good cause to believe that it will have jurisdiction over all parties thereto; the Complaint states a

claim upon relief may be granted against Defendants under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125), common law trespass to chattels, unjust enrichment, conversion, and negligence.

2. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125), common law trespass to chattels, unjust enrichment, conversion, and negligence, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. There is good cause to believe that, unless the Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125), common law trespass to chattels, unjust enrichment, conversion, and negligence. The evidence set forth in Microsoft's Brief in Support of Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Motion"), and the accompanying declarations and exhibits, demonstrates that Microsoft is likely to prevail on its claim that Defendants have engaged in violations of the foregoing law by:

- a. intentionally accessing and sending malicious code to Microsoft's and its customers' protected computers and operating systems, without authorization, in order to infect those computers and make them part of the botnet;
- b. sending malicious code to configure, deploy and operate a botnet;
- c. sending unsolicited spam email to Microsoft's Hotmail accounts;
- d. collecting personal information, including personal email addresses; and
- e. delivering malicious code.

4. There is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft, its customers, and the public. There is good cause to believe that the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court;

5. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of the IP addresses and Internet domains at issue in Microsoft's TRO Motion and other discoverable evidence of Defendants' misconduct available through such IP addresses and Internet domains if the Defendants receive advance notice of this action. Based on the evidence cited in Microsoft's TRO Motion and accompanying declarations and exhibits, Microsoft is likely to be able to prove that:

- a. Defendants are engaged in activities that directly violate United States law and harms Microsoft, its customers and the public;
- b. Defendants have continued their unlawful conduct despite the clear injury to Microsoft, its customers, and the public;
- c. Defendants are likely to relocate the information and evidence of their misconduct stored at the IP addresses and Internet domains at issue in Microsoft's TRO Motion and the harmful and malicious code disseminated through these IP addresses and Internet domains; and
- d. Defendants are likely to warn its associates engaged in such activities if informed of Microsoft's action.

6. Microsoft's request for this emergency *ex parte* relief is not the result of any lack of diligence on Microsoft's part, but instead based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), Civil L.R. 65-1 and the All-Writs Act, 28 U.S.C. § 1651, good cause and the interest of justice require that this Order be Granted without prior notice to Defendants, and accordingly, Microsoft is relieved of the duty to provide Defendants with prior notice of Microsoft's motion;

7. There is good cause to believe that Defendants have engaged in illegal activity using the IP addresses and the .com and .cc domains that are maintained by the top level domain registry Verisign, located in the United States and the Eastern District of Virginia.

8. There is good cause to believe that to immediately halt the injury caused by Defendants, the hosting companies, IP registries, domain registries and domain registrars set forth in Appendices A and B, must be ordered, at 3:00 a.m. Eastern Daylight Time on September 26, 2011 or such other date and time as requested by Microsoft within seven days of this Order:

- a. to immediately take all steps necessary to lock at the registry level the domains at issue in the TRO Motion, and which are set forth at Appendix A hereto, to ensure that changes to the domain names cannot be made absent a court order;
- b. to immediately take all steps required to propagate the foregoing domain registry changes to domain name registrars; and
- c. to hold the domains in escrow and take all steps necessary to ensure that the evidence of misconduct available through the domains be preserved.
- d. to immediately take all steps necessary to disable access to the IP addresses at issue in the TRO Motion, and which are set forth at Appendix B hereto, to ensure that access to the IP addresses cannot be made absent a court order;

9. There is good cause to permit notice of the instant order, notice of the Preliminary Injunction hearing and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, satisfy Fed. R. Civ. Pro. 4(f)(3) and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided contact information in foreign countries that are signatory to such treaties, (3) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their domain name registrars and as agreed to

by Defendants in their domain name registration agreements, (4) publishing notice on a publically available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

IT IS THEREFORE ORDERED that, Defendants and their representatives are temporarily restrained and enjoined from intentionally accessing and sending malicious software or code to Microsoft's and its customers protected computers and operating systems, without authorization, in order to infect those computers and make them part of the Kelihos botnet, sending malicious code to configure, deploy and operate a botnet, sending unsolicited spam email to Microsoft's email and messaging accounts and services, sending unsolicited spam email that falsely indicates that they originated from Microsoft or are approved by Microsoft or are from its email and messaging accounts or services, collecting personal information including personal email addresses, delivering malicious code including fake antivirus software, or undertaking similar activity that inflicts harm on Microsoft, its customers, or the public.

IT IS FURTHER ORDERED that, Defendants and their representatives are temporarily restrained and enjoined from configuring, deploying, operating or otherwise participating in or facilitating the botnet described in the TRO Motion, including but not limited to the command and control software hosted at and operating through the IP addresses and domains set forth herein and through any other component or element of the botnet in any location.

IT IS FURTHER ORDERED that Defendants and their representatives are temporarily restrained and enjoined from using the "Microsoft," "Windows," "Hotmail," "Windows Live" and "MSN" trade names, trademarks or service marks, in Internet Domain addresses or names, in content or in any other infringing manner or context, or acting in any other manner which suggests in any way that Defendants' products or services come from or are somehow sponsored or affiliated with Microsoft, and from otherwise unfairly competing with Microsoft, misappropriating that which rightfully belongs to Microsoft, or passing off their goods as Microsoft's.

IT IS FURTHER ORDERED that the domain registries and registrars set forth in Appendix A must:

- a. immediately take all steps necessary to lock at the registry level the domains at issue in the TRO Motion, an which are set forth at Appendix A hereto, to ensure that changes to the domain names cannot be made absent a court order;
- b. immediately take all steps required to propagate to the foregoing domain registry changes to domain name registrars; and
- c. hold the domains in escrow and take all steps necessary to ensure that the evidence of misconduct available through the domains be preserved.
- d. Shall completely refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and shall refrain from publicizing this Order until this Order is executed in full, except as explicitly provided for in this Order;
 - a. Shall save all communications to or from Defendants or Defendants' Representatives and/or related to the domains set forth in Appendix A;
 - c. Shall preserve and retain all records and documents associated with Defendants' or Defendants' Representatives' use of or access to the domains set forth in Appendix A, including billing and contact information relating to the Defendants or Defendants' representatives using these servers and all logs associated with these servers.

IT IS FURTHER ORDERED that the Internet hosting and service providers identified in Appendix B to this order:

- b. Shall immediately take all reasonable steps necessary to completely block all access by Defendants, Defendants' representatives, resellers, and any other person or computer to the IP addresses set forth in Appendix B, except as explicitly provided for in this Order;

- c. Shall immediately and completely disable the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with the IP addresses set forth in Appendix B and make them inaccessible from any other computer on the Internet, any internal network, or in any other manner, to Defendants, Defendants' representatives and all other persons, except as otherwise ordered herein;
- d. Shall immediately, completely, and until further order of this Court, suspend all services associated with the IP addresses set forth in Appendix B;
- e. Shall not enable, and shall take all reasonable steps to prevent, any circumvention of this order by Defendants or Defendants' representatives associated with the IP addresses or any other person;
- f. Shall disable, and shall deny to Defendants and Defendants' representatives, access to any and all "backup" systems, arrangements or services that might otherwise be used to support the IP addresses set forth in Appendix B or that might otherwise be used to circumvent this Order;
- g. Shall log all attempts to connect to or communicate with the IP addresses set forth in Appendix B;
- h. Shall save all communications to or from Defendants or Defendants' Representatives and/or related to the IP addresses set forth in Appendix B;
- i. Shall preserve and retain all records and documents associated with Defendants' or Defendants' Representatives' use of or access to the IP addresses set forth in Appendix B, including billing and contact information relating to the Defendants or Defendants' representatives using these servers and all logs associated with these servers;
- j. Shall completely refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and

shall refrain from publicizing this Order until this Order is executed in full, except as explicitly provided for in this Order;

IT IS FURTHER ORDERED that Internet hosting and service providers identified in Appendix B to this Order:

- a. Shall immediately identify and create a written list of domains, if any, hosted at the IP addresses set forth in Appendix B; shall transfer any content and software associated with such domains to IP addresses not listed in Appendix B; and shall notify the domain owners of the new IP addresses, and direct the domain owners to contact Microsoft's Counsel, Gabriel M. Ramsey, Orrick Herrington & Sutcliffe, 1000 Marsh Road, Menlo Park, CA 90425-1015, (Tel: 650-614-7400), to facilitate any follow-on action.
- b. Shall produce to Microsoft documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling the IP addresses set forth in Appendix B, including any and all individual or entity names, mailing addresses, e-mail addresses, facsimile numbers and telephone numbers or similar contact information, including but not limited to such contact information reflected in billing, usage and contact records.

IT IS FURTHER ORDERED that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means authorized by law, including (1) by personal delivery upon defendants who provided contact information in the U.S.; (2) personal delivery through the Hague Convention on Service Abroad upon defendants who provided contact information outside the U.S.; (3) by transmission by e-mail, facsimile and mail to the contact information provided by defendants to the data centers, Internet hosting providers and domain registrars who hosted the software code associated with the domains and IP addresses set forth at Appendices A and B; and (4) by

publishing notice to Defendants on a publicly available Internet website and/or in newspapers in the communities in which Defendants are believed to reside.

IT IS FURTHER ORDERED, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before this Court ^{on October 5th 2011 at 10:30 AM} ~~within 14 days from the date of this order.~~ to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against the Defendants, enjoining them from the conduct temporarily restrained by the preceding provisions of this Order.

IT IS FURTHER ORDERED that Microsoft shall post bond in the amount of \$10,000 as cash to be paid into the Court registry.

IT IS FURTHER ORDERED that the Defendants shall file with the Court and serve on Microsoft's counsel any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later than four (4) days prior to the hearing on Microsoft's request for a preliminary injunction. Microsoft may file responsive or supplemental pleadings, materials, affidavits, or memoranda with the Court and serve the same on counsel for the Defendants no later than one (1) day prior to the preliminary injunction hearing in this matter. Provided that service shall be performed by personal or overnight delivery, facsimile or electronic mail, and documents shall be delivered so that they shall be received by the other parties no later than 4:00 p.m. (Eastern Standard Time) on the appropriate dates listed in this paragraph.

IT IS SO ORDERED
Entered this 22nd day of September, 2011.

10:14 A.M.
E.D.T.

/s/
James C. Cacheris
United States District Judge
United States District Judge

EXHIBIT 17.

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division**

MICROSOFT CORPORATION, a
Washington corporation,

Plaintiff,

v.

DOMINIQUE ALEXANDER PIATTI, an
individual; DOTFREE GROUP S.R.O., a
Czech limited liability company, JOHN
DOES 1-22, CONTROLLING A
COMPUTER BOTNET THEREBY
INJURING MICROSOFT AND ITS
CUSTOMERS

Defendants.

Civil Action No: 1:11cv1017 (JCC/IDD)

CONSENT PRELIMINARY INJUNCTION

Plaintiff Microsoft Corp. ("Microsoft") has filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) the CAN-SPAM Act (15 U.S.C. § 7704); (3) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); and (4) the common law of trespass, unjust enrichment, conversion, and negligence. Microsoft has moved for a preliminary injunction pursuant to Rule 65(b) of the Federal Rules of Civil Procedure and the All-Writs Act, 28 U.S.C. § 1651.

FINDINGS

Findings Regarding The Domain "CZ.CC"

With respect to the internet domain name "cz.cc," one of the domains that is the subject of Microsoft's motion for a preliminary injunction, the Court makes the following findings:

1. Plaintiff Microsoft and Defendants Dominique Piatti and dotFree Group s.r.o., have jointly advised the Court that the parties have reached agreement regarding the disposition of the "cz.cc" domain during the pendency of this action. Microsoft, Dominique Piatti and

dotFree Group have specifically advised the Court that such agreement includes provisions to disable malicious subdomains and a process to verify the identities of sub-domain registrants, and that Mr. Piatti and dotFree Group s.r.o. desire to comply with and adhere to the terms of that agreement and this Order.

2. Plaintiff Microsoft and Defendants Dominique Piatti and dotFree Group s.r.o. have jointly advised the Court that the parties stipulate to the Court's jurisdiction and authority to enter the relief set forth herein regarding the domain "cz.cc," without waiver of any of the parties' rights or positions in this action.

Findings Regarding Domains Registered By John Doe Defendants

The Court has considered the pleadings, declarations, exhibits, and memorandum filed in support of Microsoft's motion and finds, with respect to Defendants John Does 1-22 that:

1. This Court has jurisdiction over the subject matter of this case and there is good cause to believe that it will have jurisdiction over all parties thereto; the Complaint states a claim upon which relief may be granted against John Doe Defendants under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125), common law trespass to chattels, unjust enrichment, conversion, and negligence;

2. There is good cause to believe that John Doe Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125), common law trespass to chattels, unjust enrichment, conversion, and negligence, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. There is good cause to believe that, unless the John Doe Defendants are enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham

Act (15 U.S.C. § 1125), common law trespass to chattels, unjust enrichment, conversion, and negligence. The evidence set forth in Microsoft's Brief in Support of Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Motion"), and the accompanying declarations and exhibits, demonstrates that Microsoft is likely to prevail on its claim that John Doe Defendants have engaged in violations of the foregoing law by:

- a. intentionally accessing and sending malicious code to Microsoft's and its customers' protected computers and operating systems, without authorization, in order to infect those computers and make them part of the botnet;
- b. sending malicious code to configure, deploy and operate a botnet;
- c. sending unsolicited spam email to Microsoft's Hotmail accounts;
- d. collecting personal information, including personal email addresses; and
- e. delivering malicious code.

4. There is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft, its customers, and the public. There is good cause to believe that the John Doe Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court;

5. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by John Doe Defendants of the Internet domains at issue in Microsoft's Motion for Preliminary Injunction and other discoverable evidence of John Doe Defendants' misconduct available through such Internet domains if the John Doe Defendants receive advance notice of this action. Based on the evidence cited in Microsoft's Motion for Preliminary Injunction and accompanying declarations and exhibits, Microsoft is likely to be able to prove that:

- a. John Doe Defendants are engaged in activities that directly violate United States law and harms Microsoft, its customers and the public;

- b. John Doe Defendants have continued their unlawful conduct despite the clear injury to Microsoft, its customers, and the public;
- c. John Doe Defendants are likely to relocate the information and evidence of their misconduct stored at the Internet domains at issue in Microsoft's Motion and the harmful and malicious code disseminated through these Internet domains; and
- d. John Doe Defendants are likely to warn its associates engaged in such activities if informed of Microsoft's action.

6. Microsoft's request for this emergency *ex parte* relief is not the result of any lack of diligence on Microsoft's part, but instead based upon the nature of John Doe Defendants' unlawful conduct.

7. There is good cause to believe that John Doe Defendants have engaged in illegal activity using domains that are maintained by the top level domain registry Verisign, located in the United States and the Eastern District of Virginia.

8. There is good cause to believe that to immediately halt the injury caused by John Doe Defendants, the domain registries and domain registrars set forth in Appendix A in relation to all domains other than cz.cc, must be ordered:

- a. to immediately take all steps necessary to lock at the registry level and to place on registry hold all of the domains set forth at Appendix A hereto (except for "cz.cc"), to ensure that such domains are disabled during the pendency of this action and that changes to the domain names cannot be made absent a court order;
- b. to immediately take all steps required to propagate the foregoing domain registry changes to domain name registrars; and
- c. to hold the domains in escrow and take all steps necessary to ensure that the evidence of misconduct available through the domains be preserved.

9. There is good cause to permit notice of the instant order and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due

Process, satisfy Fed. R. Civ. Pro. 4(f)(3) and are reasonably calculated to notify Defendants of the instant order and of this action: (1) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided contact information in foreign countries that are signatory to such treaties, (2) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their domain name registrars and as agreed to by Defendants in their domain name registration agreements, (3) publishing notice on a publically available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

PRELIMINARY INJUNCTION

IT IS THEREFORE ORDERED that Plaintiff Microsoft and Defendants Dominique Piatti and dotFree Group s.r.o. are directed to adhere strictly to the terms of the agreement between them regarding disposition of the domain “cz.cc” during the pendency of this action, to prevent the irreparable harm that has been caused by others through the “cz.cc” internet domain name. In particular, Plaintiff Microsoft and Defendants Dominique Piatti and dotFree Group are directed to adhere strictly to the provisions of the agreement regarding disablement of malicious subdomains and provisions concerning a process to verify the identities of sub-domain registrants.

IT IS THEREFORE ORDERED that, John Doe Defendants and their representatives are temporarily restrained and enjoined from intentionally accessing and sending malicious software or code to Microsoft’s and its customers protected computers and operating systems, without authorization, in order to infect those computers and make them part of the Kelihos botnet, sending malicious code to configure, deploy and operate a botnet, sending unsolicited spam email to Microsoft’s email and messaging accounts and services, sending unsolicited spam email that falsely indicates that they originated from Microsoft or are approved by Microsoft or are from its email and messaging accounts or services, collecting personal information including personal email addresses, delivering malicious code including fake antivirus software, or undertaking similar activity that inflicts harm on Microsoft, its customers, or the public.

IT IS FURTHER ORDERED that, John Doe Defendants and their representatives are temporarily restrained and enjoined from configuring, deploying, operating or otherwise participating in or facilitating the botnet described in the TRO Motion, including but not limited to the command and control software hosted at and operating through the domains set forth herein and through any other component or element of the botnet in any location.

IT IS FURTHER ORDERED that John Doe Defendants and their representatives are temporarily restrained and enjoined from using the “Microsoft,” “Windows,” “Hotmail,” “Windows Live” and “MSN” trade names, trademarks or service marks, in Internet Domain addresses or names, in content or in any other infringing manner or context, or acting in any other manner which suggests in any way that John Doe Defendants’ products or services come from or are somehow sponsored or affiliated with Microsoft, and from otherwise unfairly competing with Microsoft, misappropriating that which rightfully belongs to Microsoft, or passing off their goods as Microsoft’s.

IT IS FURTHER ORDERED that the domain registries and registrars set forth in Appendix A must:

- a. immediately take all steps necessary to lock at the registry level and to place on registry hold all of the domains set forth at Appendix A hereto (except for “cz.cc”), to ensure that such domains are disabled during the pendency of this action and that changes to the domain names cannot be made absent a court order;
- b. to immediately take all steps required to propagate the foregoing domain registry changes to domain name registrars; and
- c. to hold the domains in escrow and take all steps necessary to ensure that the evidence of misconduct available through the domains be preserved.
- d. Shall save all communications to or from Defendants or Defendants’ Representatives and/or related to the domains set forth in Appendix A;
- e. Shall preserve and retain all records and documents associated with Defendants’ or Defendants’ Representatives’ use of or access to the domains set forth in


Appendix A, including billing and contact information relating to the Defendants or Defendants' representatives using these servers and all logs associated with these servers.

IT IS FURTHER ORDERED that copies of this Order and service of the Complaint may be served by any means authorized by law, including (1) by personal delivery upon defendants who provided contact information in the U.S.; (2) personal delivery through the Hague Convention on Service Abroad upon defendants who provided contact information outside the U.S.; (3) by transmission by e-mail, facsimile and mail to the contact information provided by defendants to domain registrars through which the domains set forth at Appendix A were registered; and (4) by publishing notice to Defendants on a publicly available Internet website and/or in newspapers in the communities in which Defendants are believed to reside.

IT IS FURTHER ORDERED that Microsoft shall post bond in the amount of \$10,000 as cash to be paid into the Court registry.


IT IS SO ORDERED

Entered this 12 day of October, 2011.

 /s/
James C. Cacheris
United States District Judge

James C. Cacheris
United States District Judge

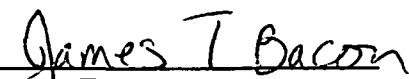
WE ASK FOR THIS:


REBECCA L. MROZ
Va. State Bar No. 77114
CHRISTOPHER M. O'CONNELL
Va. State Bar No. 65790
Attorneys for Plaintiff Microsoft Corp.
ORRICK, HERRINGTON & SUTCLIFFE LLP
1152 15th Street, N.W.
Washington, D.C. 20005-1706
Telephone: (202) 339-8400
Facsimile: (202) 339-8500
bmroz@orrick.com
coconnell@orrick.com

Of counsel:

GABRIEL M. RAMSEY (*pro hac vice*)
JACOB M. HEATH (*pro hac vice*)
Attorneys for Plaintiff Microsoft Corp.
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401
gramsey@orrick.com
jheath@orrick.com

Counsel for Plaintiff Microsoft Corp.


James T. Bacon
Va. Bar No. 22146
Warner F. Young, III
Va. Bar No. 24259
Attorneys for Defendants Dominique A. Piatti and dotFree Group s.r.o.
Allred, Bacon, Halfhill & Young, PC
11350 Random Hills Road, Ste. 700
Fairfax, Virginia 22030
Tel.: (703) 352-1300
Fax: (703) 352-1301
jbacon@abhylaw.com
wyoung@abhylaw.com

Counsel for Defendants Dominique A. Piatti
and dotFree Group s.r.o.

APPENDIX A

Domain Names Of Command And Control Servers	Domain Registry And Registrars	Registrant Information
cz.cc	<p>Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166</p> <p>Moniker Online Services, Inc. / Moniker Online Services LLC 20 SW 27th Ave, Suite 201 Pompano Beach, Florida 33069</p>	<p>Dominique Alexander Piatti dotFree Group s.r.o. Prazska 636 Dolni Brezany Praha-Zapad 25241 Czech Republic domi@cz.cc</p> <p>Dominique Piatti Postfach 127 Guemligen Bern 3073 Switzerland Dominique_piatti@hotmail.com</p>
bricord.com	<p>Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois bricord.com c/o bricord.com N4892 Nassau Bahamas flyz0mt4db6aa1b61833@oqijj874d9300d54bd95.privatewhois.net oq9wmmx4db6aa1b6b08e@oqijj874d9300d54bd95.privatewhois.net n8h23tc4db6aa1b675f5@oqijj874d9300d54bd95.privatewhois.net</p>
bevvyky.com	<p>Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois bevvyky.com c/o bevvyky.com N4892 Nassau Bahamas nomklo44e314f83cfc56@oqijj874d9300d54bd95.privatewhois.net c6e5z0k4e314f83d3306@oqijj874d9300d54bd95.privatewhois.net kh91bdf4e314f83d2364@oqijj874d9300d54bd95.privatewhois.net</p>
carbili.com	<p>Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois carbili.com c/o carbili.com N4892 Nassau Bahamas Int5fmm4da33006da6ad@oqijj874d9300d54bd95.privatewhois.net hh7429m4da33006dc6f3@oqijj874d9300d54bd95.privatewhois.net e2m0ez64da33006dbb39@oqijj874d9300d54bd95.privatewhois.net</p>

codfirm.com	<p>Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois codfirm.com c/o codfirm.com N4892 Nassau Bahamas</p> <p>hzteezh4da5e55a43a3f@oqij874d9300d54bd95.privatewhois.net otqbyon4da5e55a480d4@oqij874d9300d54bd95.privatewhois.net klwwh2i4da5e55a449e3@oqij874d9300d54bd95.privatewhois.net</p>
dissump.com	<p>Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois dissump.com c/o dissump.com N4892 Nassau Bahamas</p> <p>itamzr14da5e558b33c0@oqij874d9300d54bd95.privatewhois.net yvamaby4da5e558ba4dc@oqij874d9300d54bd95.privatewhois.net hwhmpus4da5e558b952a@oqij874d9300d54bd95.privatewhois.net</p>
doloas.com	<p>Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois doloas.com c/o doloas.com N4892 Nassau Bahamas</p> <p>sk2xcdp4db6aa1e1a72d@oqij874d9300d54bd95.privatewhois.net satosfb4db6aa1e1c673@oqij874d9300d54bd95.privatewhois.net ka94bx44db6aa1e1b6f3@oqij874d9300d54bd95.privatewhois.net</p>
editial.com	<p>Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois editial.com c/o editial.com N4892 Nassau Bahamas</p> <p>ugz6k834db6aa1bdf3db@oqij874d9300d54bd95.privatewhois.net klabhbh4db6aa1be12f3@oqij874d9300d54bd95.privatewhois.net w5n0ngq4db6aa1be078a@oqij874d9300d54bd95.privatewhois.net</p>
gratima.com	<p>Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois gratima.com c/o gratima.com N4892 Nassau Bahamas</p> <p>nmpzuvs4db6aa1e9484b@oqij874d9300d54bd95.privatewhois.net ecvgjy74db6aa1e9a9e9@oqij874d9300d54bd95.privatewhois.net vmjy2s54db6aa1e99a3f@oqij874d9300d54bd95.privatewhois.net</p>
hellohello123.com	<p>Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166</p>	<p>Verisign Naming Services Attn: VNDS Monitoring-East 21345 Ridgetop Circle 4th Floor</p>

	Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Dulles, Virginia 20166
knifell.com	Verisign Naming Services 21345 Ridgetop Circle 4 th Floor Dulles, Virginia 20166 Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois knifell.com c/o knifell.com N4892 Nassau Bahamas nff7lac4db6aa1c5f12f@oqijj874d9300d54bd95.privatewhois.net f9rcd314db6aa1c61040@oqijj874d9300d54bd95.privatewhois.net xxjkjti4db6aa1c60486@oqijj874d9300d54bd95.privatewhois.net
lalore.com	Verisign Naming Services 21345 Ridgetop Circle 4 th Floor Dulles, Virginia 20166 Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois lalore.com c/o lalore.com N4892 Nassau Bahamas q5sgyzx4da5e55aba0cb@oqijj874d9300d54bd95.privatewhois.net gh8xk5h4da5e55abbclc@oqijj874d9300d54bd95.privatewhois.net fmci3dk4da5e55abb06l@oqijj874d9300d54bd95.privatewhois.net
magdali.com	Verisign Naming Services 21345 Ridgetop Circle 4 th Floor Dulles, Virginia 20166 Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois magdali.com c/o magdali.com N4892 Nassau Bahamas n0vo7qm4da5e55b7a19l@oqijj874d9300d54bd95.privatewhois.net bvdkatd4da5e55b82230@oqijj874d9300d54bd95.privatewhois.net wl505fm4da5e55b80ee3@oqijj874d9300d54bd95.privatewhois.net
partric.com	Verisign Naming Services 21345 Ridgetop Circle 4 th Floor Dulles, Virginia 20166 Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois partric.com c/o partric.com N4892 Nassau Bahamas rsjyi9e4db6aa1d28df3@oqijj874d9300d54bd95.privatewhois.net t9js2644db6aa1d2d019@oqijj874d9300d54bd95.privatewhois.net fv88khq4db6aa1d2c0ba@oqijj874d9300d54bd95.privatewhois.net
restonal.com	Verisign Naming Services 21345 Ridgetop Circle 4 th Floor Dulles, Virginia 20166 Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois restonal.com c/o restonal.com N4892 Nassau Bahamas uuyidk54da5e55939e3c@oqijj874d9300d54bd95.privatewhois.net cqvb1nj4da5e5593f00f@oqijj874d9300d54bd95.privatewhois.net ck1u2t54da5e5593e0be@oqijj874d9300d54bd95.privatewhois.net

subcosi.com	Verisign Naming Services 21345 Ridgetop Circle 4 th Floor Dulles, Virginia 20166 Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois subcosi.com c/o subcosi.com N4892 Nassau Bahamas lz0xca94da5e559c6462@oqij874d9300d54bd95.privatewhois.net typqrv4da5e559c8f22@oqij874d9300d54bd95.privatewhois.net zzhu7vv4da5e559c7b9b@oqij874d9300d54bd95.privatewhois.net
uncter.com	Verisign Naming Services 21345 Ridgetop Circle 4 th Floor Dulles, Virginia 20166 Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois uncter.com c/o uncter.com N4892 Nassau Bahamas cv47vjf4da5e55be3901@oqij874d9300d54bd95.privatewhois.net cgvnijf4da5e55be5bfl@oqij874d9300d54bd95.privatewhois.net lkvy5fh4da5e55be4c53@oqij874d9300d54bd95.privatewhois.net
wargalo.com	Verisign Naming Services 21345 Ridgetop Circle 4 th Floor Dulles, Virginia 20166 Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois wargalo.com c/o wargalo.com N4892 Nassau Bahamas dy0stoh4db6aa1da2eda@oqij874d9300d54bd95.privatewhois.net o2jtp64db6aa1da7522@oqij874d9300d54bd95.privatewhois.net ty3s2ct4db6aa1da6199@oqij874d9300d54bd95.privatewhois.net
wormetal.com	Verisign Naming Services 21345 Ridgetop Circle 4 th Floor Dulles, Virginia 20166 Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois wormetal.com c/o wormetal.com N4892 Nassau Bahamas u5248i34db6aa1f24b3c@oqij874d9300d54bd95.privatewhois.net bjhl1334db6aa1f27244@oqij874d9300d54bd95.privatewhois.net oykewjr4db6aa1f25efl@oqij874d9300d54bd95.privatewhois.net
earplat.com	Verisign Naming Services 21345 Ridgetop Circle 4 th Floor Dulles, Virginia 20166 Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois earplat.com c/o earplat.com N4892 Nassau Bahamas x1giip14e315630344b@oqij874d9300d54bd95.privatewhois.net o4yns8o4e315631095bd@oqij874d9300d54bd95.privatewhois.net sbh8ipe4e31563107e77@oqij874d9300d54bd95.privatewhois.net
metapli.com	Verisign Naming Services 21345 Ridgetop Circle 4 th Floor Dulles, Virginia 20166	Private Whois metapli.com c/o metapli.com N4892 Nassau Bahamas

	Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	pzjjnfc4e3155e157ceb@oqjj874d9300d54bd95.privatewhois.net yeij2yh4e3155e15b733@oqjj874d9300d54bd95.privatewhois.net zv2ea6o4e3155e15a79a@oqjj874d9300d54bd95.privatewhois.net
--	--	--

EXHIBIT 18.



Source: Privacy & Security Law Report: News Archive > 2012 > 03/05/2012 > Conference Report: RSA Conference 2012 > Internet: White House Advisor Schmidt Discusses Online Trusted ID Plan, Fighting Botnets

11 PVLR 404

Internet

White House Advisor Schmidt Discusses Online Trusted ID Plan, Fighting Botnets

By Joyce E. Cutler

SAN FRANCISCO—The private sector is going to be in the driver's seat for creating a framework for trusted identities in online transactions, White House Cybersecurity Coordinator Howard Schmidt said Feb. 29.

Schmidt, speaking at a session of the RSA Conference 2012, said that the core of the administration's National Strategy for Trusted Identities in Cyberspace (NSTIC) is to make sure individuals, businesses, and computer-to-computer activities can use interoperable digital credentials.

The cybersecurity chief stressed that the framework will draw on industry expertise and the marketplace to have online identities validated and privacy protections addressed.

"The government will be and is a consumer of this technology and not the one that is going to go out and build this. Government should not be in that business. It's not the core competency. It's not the role of the government, but clearly it's the idea of the marketplace being driven by innovators and entrepreneurs," Schmidt said.

In April 2011, the Obama White House released its final draft of the NSTIC, which it said is designed to make internet communications and transactions more secure to reduce fraud and identity theft (10 PVLR 618, 4/25/11).

The private sector will build it "so we can get out of this massive, expensive, password management environment that we live in today," Schmidt said.

Moving Against Botnets

The Commerce Department's National Institute of Standards and Technology and the Department of Homeland Security are teaming up with the private sector to look at a voluntary industry code of conduct to address detection and shutdown of botnets (10 PVLR 1377, 9/26/11).

Botnets are networks of infected computers used to launch malicious denial of service attacks, send spam, and store illegal content.

Australia through its internet association has an "iCode" of conduct with its internet service providers to reduce these so-called "zombie" attacks, Schmidt noted. While Australia is still developing statistics about how effective the code is, "the bottom line is if we have 5 percent less botnets, that's better than where we are today," he said.

Industry has raised concerns that owners and operators would be opening themselves to more government regulation, Schmidt said.

"None of us can predict what somebody might think about in the future," he said. "But what we need to make sure is what we're doing right now is [that] we're doing what we can to reduce the likelihood [of a successful cyber-attack], so it doesn't give someone in the future ammunition to say [that the] 'private sector is not responding.'"

White House Cybersecurity Plan

In June 2011, Commerce release a final draft paper developing cybersecurity strategies for non-covered critical infrastructure (10 PVLR 871, 6/13/11), Ari Schwartz, NIST senior internet policy adviser said.

He added that "no one right now is suggesting regulating, but yet there's an acknowledgment there are security issues at hand."

BNA INSIGHTS ARCHIVE

Building an Online
Identity Legal
Framework: The Proposed
National Strategy—
Thomas J. Smedinghoff,
Wildman Harrold, Chicago

Within the next 90 days, the government is going to ask its private sector partners to roll out the framework addressing the issue and “develop the group that will lead this thing going forward,” Schmidt said.

“This is not something we're going to continue to sit by and watch. We know it's out there. We've admired the problem long enough. It's time to act on it. We have the right people, the right stakeholders, the right leaders on the government side to help facilitate it, and I think it's going to move forward in a rapid manner,” Schmidt predicted.

For More Information

Further information on the RSA Conference 2012 is available at <http://365.rsaconference.com/index.jspa>.

Contact us at <http://www.bna.com/contact/index.html> or call 1-800-372-1033

ISSN 1538-3431

Copyright © 2012, The Bureau of National Affairs, Inc.. Reproduction or redistribution, in whole or in part, and in any form, without express written permission, is prohibited except as permitted by the BNA Copyright Policy. <http://www.bna.com/corp/index.html#V>

EXHIBIT 19.

Guidance for Preparing Domain Name Orders, Seizures & Takedowns

Abstract

This “thought paper” offers guidance for anyone who prepares an order that seeks to seize or take down domain names. Its purpose is to help preparers of legal or regulatory actions understand what information top level domain name (TLD) registration providers such as registries and registrars will need to respond promptly and effectively to a legal or regulatory order or action. The paper explains how information about a domain name is managed and by whom. In particular, it explains that a seizure typically affects three operational elements of the Internet name system – domain name registration services, the domain name system (DNS) and WHOIS services – and encourages preparers of legal or regulatory actions to consider each when they prepare documentation for a court action.

Table of Contents

GUIDANCE FOR PREPARING DOMAIN NAME ORDERS, SEIZURES & TAKEDOWNS	1
PURPOSE OF THIS PAPER	2
WHAT INFORMATION SHOULD ACCOMPANY A LEGAL OR REGULATORY ORDER OR ACTION?	4
CHECKLIST OF INFORMATION TO SUBMIT WITH A LEGAL OR REGULATORY ACTION .	5
ADDITIONAL CONSIDERATIONS.....	12
CONTACT US	13
REFERENCES.....	16

Purpose of this paper

Recent legal actions resulting in disrupting or dismantling major criminal networks (Rustockⁱ, Corefloodⁱⁱ, Kelihosⁱⁱⁱ) have involved seizures of domain names, domain name system (DNS) name server reconfiguration, and transfers of domain name registrations as part of the take down actions. These activities have been taken to mitigate criminal activities and will likely continue to be elements of future anticrime efforts.

Generally, court-issued seizure warrants or restraining orders in the United States or similar governmental jurisdictions identify the required, immediate actions a party must take and accompany these with sufficient information for domain name registration providers such as registry operators or registrars to comply. Domain name registration providers can promptly obey complaints or legal or regulatory actions (or voluntarily cooperate with law enforcement agents and the private sector) when the instructions of the court or regulatory entity specify the immediate and long-term actions required as completely and unambiguously as possible.

Providing all of the information that registry operators or registrars need to comply with an order or request requires some familiarity with Internet protocols, technology and operations. Law enforcement agents, attorneys, officers of courts and others who are not familiar with the operation and interrelationship of domain name registration services, the domain name system (DNS), and WHOIS services can benefit from a reference list of questions and guidance for “answers” (information) that ideally would be made available when action is specified in a court order.

We offer a list of questions and encourage preparers to answer each when the legal or regulatory action seeks to seize or take down a domain name. For each question, a checklist or explanation of information that preparers should make available to registry operators or registrars is provided. Note that it may not necessarily be the case that all of the information identified in this list will be relevant for all types of seizure or take down actions.

The information discussed here is not exhaustive, nor are these questions prescriptive. However, the preparation and execution of actions or orders may be expedited if these details are considered during the preparation of a legal or regulatory action or during the onset of an incident involving the DNS, including domain name registrations.

The comments and recommendations made in here are based on experience with actions and orders that have been prepared and executed by U.S. courts. This is a lay document. Its authors and contributors are technical and operational staff, not attorneys [although persons with legal expertise were consulted in the preparation

of this document for publication]. We offer no legal advice here. Our purpose is to share “field experience” so that these can be taken into consideration for future actions and orders involving domain name seizures and take downs.

Domain name seizures are typically ordered in association with criminal acts. Preparers of orders should consider whether disputes concerning alleged abusive registrations of domain names (e.g., bad faith use, confusing similarity) may be handled through the Uniform Domain Name Dispute Resolution Policy and administrative procedure, found at [^{iv}].

ICANN Security Team

What information should accompany a legal or regulatory order or action?

Domain name registration is a multi-step process. An organization or individual that wants to use a domain name first checks availability of the string of characters in a given Top Level Domain (TLD), and if available, must register the domain name. ICANN accredited registrars process registrations for ICANN generic TLDs (gTLD). Country-specific TLDs (ccTLDs) are not under obligation to use ICANN accredited registrars and may use any registration provider or they may provide registration services directly.

A fee for a term of use is commonly paid to register a domain. Upon completing a domain name registration, the domain name is made active in the TLD registry, a registration record is created, and the Domain Name System is configured to allow name to Internet address resolution for the domain and services such as email or web. Often, several business entities coordinate to perform these actions on behalf of the registering party (the registrant) and to manage all the information associated with a domain throughout that domain's life cycle. Nearly all of this information may be relevant or essential to a successful execution of a legal or regulatory order or action.

Domain name registration providers such as registries or registrars require certain information to enable them to satisfy a court order or investigate a legal or regulatory action. As you prepare one of these documents, consider the following high-level questions:

1) Who is making the legal or regulatory action or issuing a request?

Examples: a court of law, a law enforcement agent/agency, a registry, a registrar, an attorney, or an intervener (e.g., a trusted or contracted agent of a complainant who has assisted in the technical or operational investigation of criminal activity).

2) What changes are required to the **registration** of the domain name(s) listed in the legal or regulatory order or action?

Individuals or organizations register and pay an annual fee to use a domain name. The individual or organization then becomes the *registrant on record* of the domain. Parties that perform domain name registrations as a service ("registrars" or "registries") collect contact, billing and other information from the registrant. A legal or regulatory action should describe if this information is to be altered, and how.

A domain name registration also identifies the *status* of the domain^v. Status indicates the operational state of a domain name in a registry, i.e., whether or not the domain name is active or not. Status also serves as an access control, i.e., whether or not the registration of a domain name can be transferred, modified, or deleted. A legal or regulatory order or action should specify the status a registrar or registry should assign to the domain name(s) listed in the legal or regulatory order or action. [Note that status also preserves the state of information associated with a domain name in services such as data escrow and registration data information services such as WHOIS].

In cases where the registration of a domain name is to be transferred away from a party named in a legal or regulatory action to law enforcement or an agent operating on behalf of law enforcement, the legal or regulatory action should provide the “replacement” domain name registration data as described in ICANN’s registrar accreditation agreement (RAA^{vi}).

- 3) Should the Domain Name System (DNS) continue to **resolve the domain name(s)** listed in the legal or regulatory action?

Provisions must be made in the DNS to make the name usable, i.e., to make it possible for Internet users to locate (determine the Internet address of) web, mail, or other services the registrant intends to host. The process of locating hosts using the DNS is called domain name resolution. The legal or regulatory action should indicate whether and how the DNS is to be configured, whether domain name(s) listed in the order or action are to resolve, and how.

- 4) What changes are required to the **WHOIS information** associated with the domain name(s) listed in the legal or regulatory action?

Certain information about a domain name registration – the registrant on record, point of contact information, domain status, sponsoring registrar, name server address – may be available via an Internet service called **WHOIS**. The legal or regulatory action should identify what information WHOIS services should provide in response to queries about domain name(s) identified in the legal or regulatory action.

Checklist of information to submit with a legal or regulatory action

Preparers of legal or regulatory actions are encouraged to consider whether the questions presented below have been answered in an order or action. For each question, there is an accompanying checklist or explanatory text to help preparers. The table considers a single domain. When legal or regulatory orders identify multiple domains, preparers can expedite handling of the order by grouping the domain names by Top Level Domain type (e.g., COM, NET, BIZ, INFO...).

Who is making the request?	<input type="checkbox"/> Complainant (plaintiff) <input type="checkbox"/> Respondent (defendant) <input type="checkbox"/> Court of Record
Who are the primary points of contact?	<p>Contact information for court officers, attorneys, technical/operational staff or agents, line or senior management of parties to the legal or regulatory action:</p> <ul style="list-style-type: none"> • Name • Postal address • Telephone number(s) • Fax numbers(s) • Email address(es) <p>These prove beneficial should issues be identified that require a technical or operational action, legal consultation or business decisions; in particular, call attention to any person designated as the coordinator, lead or responsible party to the action.</p> <p><i>Important:</i> Issuers of requests are encouraged to provide some form of official, verifiable contact information. Recipients of a court order may require a method to verify the legitimacy of the issuer of the request. The inability to validate a request, especially when the request comes from a foreign law enforcement agency, court, or other entity can delay action by the recipient.</p> <p><i>Indicate whether any contact information provided is to be kept confidential.</i></p>

What kind of request is this?	<p>The request should clearly indicate whether this is a court order or request for action. For example,</p> <ul style="list-style-type: none"> <input type="checkbox"/> Court order (attached) or regulatory action <input type="checkbox"/> 3rd party request for action. Examples: <ul style="list-style-type: none"> <input type="checkbox"/> Algorithmically generated domain name HOLD request <input type="checkbox"/> Child abuse material <input type="checkbox"/> Copyright infringing materials <input type="checkbox"/> Malware Command & Control host <input type="checkbox"/> ... <p>Note: 3rd party requests should be accompanied by verifiable evidence supporting the third party request.</p>
What is the expected response time?	<p><input type="checkbox"/> Date and time by which the actions indicated in the legal or regulatory action must be executed.</p> <p>Document should make clear when the actions must be executed. This is particularly important when multiple parties must coordinate execution so that their actions are “simultaneous”.</p>
Is there a desire to obtain records related to the domain at the same time the domain is seized?	<p><input type="checkbox"/> Records and documents sought</p> <p>The legal or regulatory action should list and describe all forms of records sought and indicate the span of time. Make clear whether or not the request is part of the action.</p> <p>Important: The issuer should always seek to direct requests to the party who is in possession of the information sought, especially when preparing sealed orders. For generic TLDs, registrars typically possess billing information and other customer (registrant) information that cannot be accessed using WHOIS services (e.g., information associated with privacy protection services).</p>

<p>How is the domain name registration record to be changed?</p> <p>Note: Identify all the changes ordered or requested.</p>	<p><input type="checkbox"/> change domain name registrant</p> <p>The party identified as the domain name registrant is to be changed to the party specified in the complaint. The “gaining” party may be responsible for future registration fees.</p> <p><input type="checkbox"/> Change domain name registration point of contact information as specified</p> <p>The point of contact information recorded in the domain name registration is to be changed to the contact information specified in the complaint. The legal or regulatory action should indicate how each point of contact (registrant, administrative contact, technical contact) is to be altered.</p> <p><input type="checkbox"/> Disable DNSSEC</p> <p>DNS information that has been cryptographically protected with a digital signature will be altered so that is no longer protected</p> <p><input type="checkbox"/> Replace existing DNSSEC keys with new key(s) supplied</p> <p>DNS information that has been cryptographically protected with a digital signature will be altered so that is now protected using the key(s) supplied by the requesting entity.</p>
<p>How is domain name status to be changed?</p>	<p><input type="checkbox"/> prevent transfer of domain name</p> <p><input type="checkbox"/> prevent updates to domain name registration</p> <p><input type="checkbox"/> Delete domain name</p> <p>Deleting a domain name “releases” the name into the pool of names available for registration by any party.</p>

<p>Is the domain name to be transferred to a different sponsoring registrar?</p>	<p><input type="checkbox"/> Transfer domain to new registrar specified</p> <p>If the legal or regulatory action wants the domain name transferred from the current sponsoring registrar to a registrar identified in the order or action, the requesting entity should supply the “losing” registrar and the “gaining” registrar for this action. A unique authorization code (Auth-Code) may be required for this action. This is obtained from the losing registrar and provided to the gaining registrar as proof of consent to transfer the domain name.</p>
<p>Is the party that provides name resolution service (DNS) to be changed?</p>	<p><input type="checkbox"/> Change authority for DNS</p> <p>Authority identifies the party that is responsible for managing and providing DNS for a domain name. A legal or regulatory action should identify parties that will assume authority for name resolution of domain names listed in the document.</p> <p>This is a change to the DNS configuration of the registry (TLD) zone file. Specifically, the DNS records that identify the authoritative name server(s) for the domain name must be changed to point to IP address(es) under administrative control of the parties named in the legal or regulatory action (or request).</p> <p><input type="checkbox"/> Change DNS configuration of the domain</p> <p>This is a change to the DNS configuration of the zone file for the domain specified in the order or action. Requesting entities provide this information to registrars or 3rd party DNS providers. The requesting entity should provide current and desired values for all zone data (resource records, TTL values) that is to be changed.</p>

<p>Is name resolution service (DNS) to be suspended?</p>	<p><input type="checkbox"/> Suspend name resolution (DNS): “seize and take down”</p> <p>The legal or regulatory action should specify that domain name(s) should not resolve. In this case, the TLD registry operator will take action so that the DNS will return a non-existent domain response to any queries for any delegation in this domain.</p> <p>This action implies that the domain name is to be “locked”; i.e., that no party (e.g., registrar, registrant) can modify the status and cause the DNS to resume name resolution of the domain name).</p>
<p>Is redirection to a text of notice page required?</p>	<p><input type="checkbox"/> Redirect domain name to text of notice page: “seize and post notice”</p> <p>If the requesting entity intends to post a text of notice on a web page, the legal or regulatory action should provide the domain name(s) and IP address(es) for the name server that will perform name resolution for the domain names listed in the order or action. The legal or regulatory action should indicate the intended duration of time that redirection is to be performed.</p>

<p>Is redirection of Internet hosting required?</p>	<p><input type="checkbox"/> Redirect to host operator: “seize and operate”</p> <p>If the legal or regulatory action seeks to replace an Internet host¹ with one that is operated under the requesting entity’s purview, provide the domain name(s) and IP address(es) for the name server that will perform name resolution for the domain names listed in the legal or regulatory action. In other situations, the requesting entity may seek to keep the name (and name resolution) operational. This can happen when a problematic service is operational on the same domain name that also serves non-problematic services. The legal or regulatory action should indicate the intended duration of time that redirection is to be performed.</p> <p>¹ The requesting entity may operate a “command and control (C&C)” for the purpose of monitoring or intercepting communications, substituting commands or responses or other actions to remotely disable or supervise software executing without authorization or consent on compromised computers. (Note that the requesting entity could operate any service it chooses. This will have no bearing on what information to provide to registries or registrars.</p>
<p>What should WHOIS for the domain name display?</p>	<p><input type="checkbox"/> WHOIS information display change</p> <p>The legal or regulatory action should specify the information that the registry or registrar should use in response to queries for domain name registration data via a WHOIS service (See Appendix A for an example WHOIS response).</p> <p><input type="checkbox"/> Reveal private/proxy registration</p> <p>Individuals or organizations that register domain names may pay a fee to a registrar or 3rd party to protect part or all of the information displayed via WHOIS services from display. A legal or regulatory action should indicate when it requires the disclosure of “privacy protected” registration information.</p>

Additional Considerations

The nature and complexity of domain name seizures and takedown operations has evolved over time. Moreover, as criminals have demonstrated that they will adapt to technical measures to thwart crime, they are likely to adapt as they study legal measures. This section calls attention to some of the issues that past seizures and takedown actions have exposed.

Legal or regulatory actions are typically specific with respect to the immediate obligation; for example, they will enumerate domain names, IP addresses, and equipment that are to be seized. A legal or regulatory action can be less clear with regard to how long an action is to remain ongoing, or can impose a constraint on a registry that creates an obstacle to satisfying the instructions in the order. Certain legal or regulatory actions identify domain names that are hosted in countries outside the U.S., where the offense is not against the law.

Certain legal or regulatory actions create long-term administrative responsibilities for registries; for example, if a botnet algorithmically generates domain names, a registry may need to block registrations of these names as frequently as the algorithm generates to comply with an order. The number of domain names identified in these orders can accumulate to (tens of) thousands over a span of 1-2 years (100 algorithmically generated domains per day reaches 10,000 in 3 months' time). Legal or regulatory actions do not always indicate how long seizure or hold actions are to persist. Domain seizures (holds) also demand "zero error": should any party in the chain fail to identify or block even one domain name, a botnet that was successfully contained for months can be resurrected.

Algorithmically generated domain names may also conflict with already registered domains. Registries would typically seek to protect a legitimate registrant that has the misfortune of having registered a second level label that is identical to one algorithmically generated, but if the court order seizes the domain, registries could note the conflict but ultimately would obey the order. Moreover, domain generation algorithms used in criminal activities may (are likely to) adapt to defeat blocking techniques; for example, blocking registrations may not be practical if an algorithm were to generate tens of thousands of domains per day.

Sealed court orders pose operational challenges to TLD registry operators who rely on registrars to manage registrant contact information. The order prohibits the registry to communicate with the registrar of record but the registry cannot modify the contact information unless the registrar of record is engaged.

Legal or regulatory actions may order registries, registrars, Internet (web or mail) hosting companies, and ISPs to take specified steps at a specified date and time.

Such steps require considerable coordination and preparers of legal or regulatory actions should consider how “lead” as well as “execution” time may affect outcome.

Orders can create administrative responsibilities for registrars as well (for example, inter-registrar transfers of seized domain name registrations).

Orders generally do not consider fee waivers, nor do they typically consider the ongoing financial obligation of the “gaining” registrant to pay annual domain registration fees.

Contact Us

Dave Piscitello, Senior Security Technologist at ICANN, prepared this thought paper, with the assistance of the ICANN Security Team. Information. Reviews and comments from Internet security, technical and operational community members were essential in preparing this initial paper, and the Security Team thanks all who contributed. We welcome additional comments. Please forward all comments by electronic mail to dave.piscitello@icann.org

Appendix A. Sample WHOIS response

This is a sample response to a WHOIS query. The data labels and display format varies across registries and registrars. Values for registration data elements in **BOLD** should be provided by the requesting entity.

Domain ID: D2347548-LROR
Domain Name: **ICANN.ORG**
 Created On: 1 4-Sep-1998 04:00:00 UTC
 Last Updated On: 10-Jan-2012 21:32:13 UTC
 Expiration Date: 07-Dec-2017 17:04:26 UTC
 Sponsoring Registrar: GoDaddy.com, Inc. (R91-LROR)
 Status: CLIENT DELETE PROHIBITED
 Status: CLIENT RENEW PROHIBITED
 Status: CLIENT TRANSFER PROHIBITED
 Status: CLIENT UPDATE PROHIBITED
 Status: DELETE PROHIBITED
 Status: RENEW PROHIBITED
 Status: TRANSFER PROHIBITED
 Status: UPDATE PROHIBITED
 Registrant ID: CR12376439
Registrant Name: **Domain Administrator**
Registrant Organization: ICANN
Registrant Street1: **4676 Admiralty Way #330**
Registrant City: **Marina del Rey**
Registrant State/Province: **California**
Registrant Postal Code: **90292**
Registrant Country: **US**
Registrant Phone: **+1.4242171313**
Registrant FAX: **+1.4242171313**
Registrant Email: **domain-admin@icann.org**
 Admin ID: CR12376441
Admin Name: **Domain Administrator**
Admin Organization: **ICANN**
Admin Street1: **4 676 Admiralty Way #330**
Admin City: **Marina del Rey**
Admin State/Province: **California**
Admin Postal Code: **90292**
Admin Country: **US**
Admin Phone: **+1.4242171313**
Admin FAX: **+1.4242171313**
Admin Email: **domain-admin@icann.org**
 Tech ID: CR12376440
Tech Name: **Domain Administrator**
Tech Organization: **ICANN**

Tech Street1: 4676 Admiralty Way #330
Tech City: Marina del Rey
Tech State/Province: California
Tech Postal Code: 90292
Tech Country: US
Tech Phone: +1.4242171313
Tech FAX: +1.4242171313
Tech Email: domain-admin@icann.org
Name Server: NS.ICANN.ORG
Name Server: A.IANA-SERVERS.NET
Name Server: B.IANA-SERVERS.NET
Name Server: C.IANA-SERVERS.NET
Name Server: D.IANA-SERVERS.NET
DNSSEC: Signed
DS Created 1: 26-Mar-2010 15:12:06 UTC
DS Key Tag 1: 41643
Algorithm 1: 7
Digest Type 1: 1
Digest 1: 93358db22e956a451eb5ae8d2ec39526ca6a87b9
DS Maximum Signature Life 1: 1814400 seconds
DS Created 2: 26-Mar-2010 15:12:28 UTC
DS Key Tag 2: 41643
Algorithm 2: 7
Digest Type 2: 2
Digest
2:b8ab67d895e62087f0c5fc5a1a941c67a18e4b096f6c
622aefae30dd7b1ea199
DS Maximum Signature Life 2: 1814400 seconds

References

- i Defeating Rustock in the Courts
http://www.microsoft.com/security/sir/story/default.aspx#!rustock_defeating
- ii “Coreflood” Temporary Restraining Order
http://www.fbi.gov/newhaven/press-releases/pdf/nh041311_5.pdf/at_download/file
- iii “Kelihos” ex parte temporary restraining order
<http://www.noticeofpleadings.com/images/FAC-EN.pdf>
- iv Uniform Dispute Resolution Policy and procedures
<http://www.icann.org/en/dndr/udrp/policy.htm>
- v EPP Status Codes: What do they mean and why should I know?
<http://www.icann.org/en/transfers/epp-status-codes-30jun11-en.pdf>
- vi ICANN Registrar Accreditation Agreement 21 May 2009
<http://www.icann.org/en/registrars/ra-agreement-21may09-en.htm>