UNITED STATES DISTRICT COURT
DISTRICT OF CONNECTICUT

UNITED STATES OF AMERICA,	:	
	:	
Plaintiff,	:	
	:	No. 3:11 CV 561 (VLB)
v.	:	
	:	
JOHN DOE 1, JOHN DOE 2, JOHN DOE 3, JOHN DOE 4, JOHN DOE 5, JOHN DOE 6, JOHN DOE 7, JOHN DOE 8, JOHN DOE 9, JOHN DOE 10, JOHN DOE 11, JOHN DOE 12, AND JOHN DOE 13,	:	April 11, 2011
	:	
Defendants.	:	

COMPLAINT

NOW COMES the United States of America, by and through its attorney, David B. Fein, United States Attorney for the District of Connecticut, and alleges the following:

1. This is a civil action brought under Title 18, United States Code, Sections 1345 and 2521 to enjoin the Defendants from continuing to engage in wire fraud, bank fraud, and unauthorized interception of electronic communications, in violation of Title 18, United States Code, Sections 1343, 1344, and 2511, by means of malicious computer software known as "Coreflood."

2. Coreflood is a computer virus that propagates itself among computers on a network. When a computer is infected with Coreflood, the computer can be controlled remotely by another computer, referred to herein as a "command-and-control

server" or "C&C server." An infected computer is referred to as a "bot," i.e., a software "robot."

3. A single C&C server can control millions of bots. The bots controlled by a C&C server, or by a group of related C&C servers, are referred to as a "botnet." The IP address and physical location of a C&C server can be changed; accordingly, as used herein, the "predecessors" of a C&C server refer to prior, related incarnations of a C&C server that has since been moved.

4. As of April 1, 2011, the computer servers assigned IP addresses 207.210.74.74 and 74.63.232.233 were Coreflood C&C servers. The botnet controlled by those two servers, and by their predecessors, are referred to herein as the "Coreflood Botnet."

5. As of in or about February 2010, there were approximately 2,336,542 infected computers that were, or had been, part of the Coreflood Botnet. Approximately 1,853,005 of the infected computers appear to have been located in the United States, with the remainder located in countries around the world.

6. A Coreflood bot primarily identifies and communicates with its C&C server by Internet domain name, rather than by IP address. In April 2011, bots in the Coreflood Botnet identified the C&C servers as "jane.unreadmsg.net" and "vaccina.medinnovation.org," which corresponded as of April 1, 2011 to the IP addresses 207.210.74.74 and 74.63.232.233,

respectively. The Internet domain names used to identify the C&C servers for the Coreflood Botnet are changed and updated regularly.

7. The Defendants herein are the registrants of the Internet domain names used to identify the C&C servers for the Coreflood Botnet. On information and belief, the Defendants are foreign nationals.

Jurisdiction and Venue

8. Subject matter jurisdiction lies pursuant to Title 18, United States Code, Section 1345(a)(1) and Title 28, United States Code, Sections 1331 & 1345.

9. The Defendants are subject to the personal jurisdiction of this Court, having used infected computers throughout the United States as part of the Coreflood Botnet in furtherance of their scheme to defraud.

10. Venue is proper in the District of Connecticut pursuant to Title 18, United States Code, Section 1345(a)(1) and Title 28, United States Code, Section 1391(b)(2) and (d).

The Scheme to Defraud

11. A botnet, defined herein as a large number of computers to which unauthorized, remote access has been obtained, is inherently a creature of crime. A botnet can be used for many criminal purposes, including sending spam, stealing data, and committing financial fraud. A botnet also presents a threat to

national security, because it can be used to attack and disable computers, including government computers, on the Internet.

12. The Coreflood Botnet was used, among other things, to commit financial fraud. Infected computers in the Coreflood Botnet automatically recorded the keystrokes and Internet communications of unsuspecting users, including online banking credentials and passwords. The stolen data was then sent to one or more Coreflood C&C servers, where it was stored for review by the Defendants and their co-conspirators. The Coreflood C&C servers also stored the network and operating system characteristics of the infected computers. The Defendants and their co-conspirators used the stolen data, including online banking credentials and passwords, to direct fraudulent wire transfers from the bank accounts of their victims.

13. The victims of the fraud scheme described above included, inter alia:

a. A real estate company in Michigan, from whose bank account there were fraudulent wire transfers made in a total amount of approximately $115,771;

b. A law firm in South Carolina, from whose bank account there were fraudulent wire transfers made in a total amount of approximately $78,421;

c. An investment company in North Carolina, from whose bank account there were fraudulent wire transfers made in a total amount of approximately $151,201; and

d. A defense contractor in Tennessee, from whose bank account there were fraudulent wire transfers attempted in a total amount of approximately $934,528, resulting in an actual loss of approximately $241,866.

The full extent of the financial loss caused by the Coreflood Botnet is not known, due in part to the large number of infected computers and the quantity of stolen data.

14. Even without a known financial loss, however, unsuspecting owners and users of infected computers in the Coreflood Botnet are suffering a continuing and substantial injury, because, inter alia: (a) the computers are running a malicious program that the owners and users do not know about and never intended to have running; (b) the program puts at risk the privacy and confidentiality of Internet communications, including private personal and financial information, of those computer users; and (c) the program could enable the infected computers to be used in furtherance of other criminal activity, without the knowledge of the owners or legitimate users.

The Coreflood Domains

15. As alleged previously, a Coreflood bot primarily identifies and communicates with its C&C server by Internet

domain name. Specifically, each bot has a list of built-in Internet domain names, two per month, for a period of approximately one year. The first Internet domain name is used to identify the primary C&C server; the second Internet domain name may possibly be used as an alternate means of communication or control. The list of Internet domain names is updated regularly.

16. As of April 1, 2011, the following Internet domain names were built-in to the Coreflood bots controlled by the C&C servers assigned IP addresses 207.210.74.74 and 74.63.232.233:

C&C SERVER ASSIGNED 207.210.74.74

Month	Primary Domain	Alternate Domain
1/2011	a-gps.vip-studions.net	old.antrexhost.com
2/2011	dru.realgoday.net	marker.antrexhost.com
3/2011	brew.fishbonetree.biz	spamblocker.antrexhost.com
4/2011	jane.unreadmsg.net	ads.antrexhost.com
5/2011	exchange.stafilocox.net	cafe.antrexhost.com
6/2011	ns1.diplodoger.com	coffeeshop.antrexhost.com
7/2011	a-gps.vip-studions.net	old.antrexhost.com
8/2011	dru.realgoday.net	marker.antrexhost.com
9/2011	brew.fishbonetree.biz	spamblocker.antrexhost.com
10/2011	jane.unreadmsg.net	ads.antrexhost.com
11/2011	exchange.stafilocox.net	cafe.antrexhost.com
12/2011	ns1.diplodoger.com	coffeeshop.antrexhost.com

C&C SERVER ASSIGNED 74.63.232.233

Month	Primary Domain	Alternate Domain
1/2011	taxadvice.ehostville.com	taxfree.nethostplus.net
2/2011	ticket.hostnetline.com	accounts.nethostplus.net
3/2011	flu.medicalcarenews.org	logon.nethostplus.net
		imap.nethostplus.net
4/2011	vaccina.medinnovation.org	
5/2011	ipadnews.netwebplus.net	onlinebooking.nethostplus.net
6/2011	acdsee.licensevalidate.net	imap.nethostplus.net
7/2011	wellness.hostfields.net	pop3.nethostplus.net
8/2011	savupdate.licensevalidate.net	schedules.nethostplus.net

9/2011	wiki.hostfields.net	mediastream.nethostplus.net
10/2011	taxadvice.ehostville.com	taxfree.nethostplus.net
11/2011	ticket.hostnetline.com	accounts.nethostplus.net
12/2011	flu.medicalcarenews.org	logon.nethostplus.net
		imap.nethostplus.net

(collectively, the "Coreflood Domains").

17. Each of the Coreflood Domains is capable of being used by a Coreflood bot to communicate with a C&C server. In particular, past Coreflood Domains may be used by bots that have not been properly updated. Future Coreflood Domains will be used by bots in upcoming months, unless changed by a Coreflood update.

18. In general, Internet domain names are translated into IP addresses using the Internet's Domain Name System ("DNS"), a publicly-available service integral to the operation of the Internet.

19. The registry, registrar, and DNS provider for each of the Coreflood Domains is set forth in Schedule A, where the term "registry" refers to an entity that maintains records for a class of Internet domains, including the DNS provider for each domain; the term "registrar" refers to an entity that registers domain names with a registry and maintains records associated with those domains; and "DNS provider" refers to an entity chosen by a registrant to maintain the authoritative records used by DNS to translate an Internet domain name into an IP address. The registries, registrars, and DNS providers for the Coreflood Domains are referred to herein as the "Domain Service Providers."

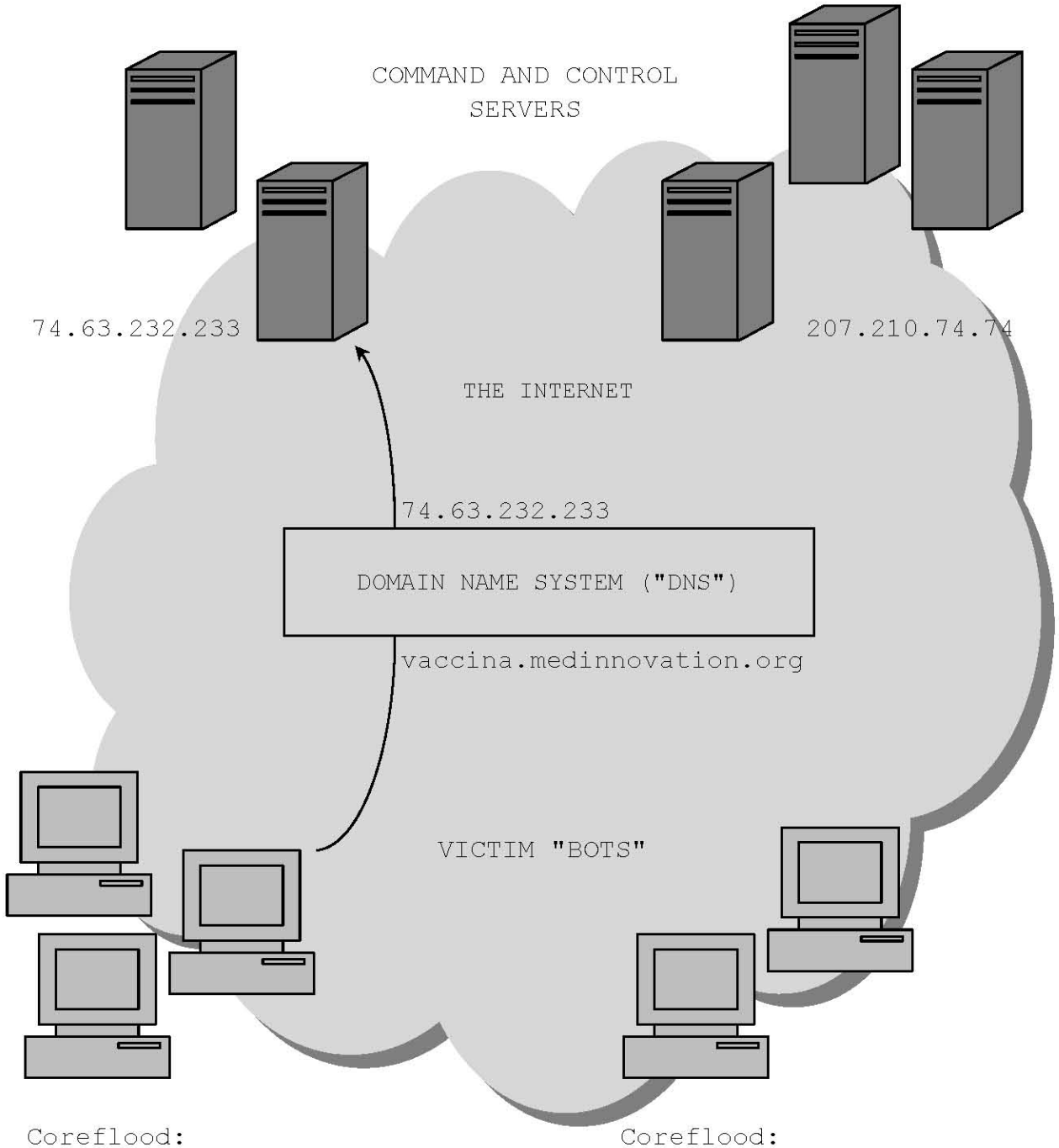
20. The Defendants registered the Coreflood Domains using stolen or fictitious identities, or using services that shield the name of the nominal registrant from public view. On information and belief, the Defendants are located outside the United States.

21. The routine operation of the Coreflood Botnet relies on services provided by the Domain Service Providers that facilitate and enable Internet communications between Coreflood bots and C&C servers.

22. When a Coreflood bot is unable to communicate with its designated C&C server, the Coreflood software will continue running on the infected computer and will periodically attempt to establish communication with a C&C server. Even after the Coreflood software is terminated, it will begin running again after certain events, such as re-starting the computer.

23. A simplified diagram of the Coreflood Botnet is shown on the next page, showing two Coreflood C&C servers and the infected computers controlled by them. The infected computers communicate with the C&C servers using built-in Coreflood Domains. One of the bots is shown beaconing to its C&C server through the Internet domain name "vaccina.medinnovation.org," which is translated by DNS into the IP address 74.63.232.233.

THE COREFLOOD BOTNET



Coreflood:
. . .
Mar 2011: flu.medicalcarenews.org
Apr 2011: vaccina.medinnovation.org
May 2011: ipadnews.netwebplus.net
. . .

Coreflood:
. . .
Mar 2011: brew.fishbonetree.biz
Apr 2011: jane.unreadmsg.net
May 2011: exchange.stafilocox.net
. . .

COUNT I

(Injunctive Relief Under 18 U.S.C. § 1345)

24. The United States of America alleges and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

25. The Defendants are engaging in wire fraud, in violation of Title 18, United States Code, Section 1343, in that the Defendants, having devised a scheme or artifice to defraud, did transmit and cause to be transmitted, by means of wire communication in interstate and foreign commerce, writings, signs, and signals for the purpose of executing such scheme or artifice.

26. Pursuant to Title 18, United States Code, Sections 1345(a)(1) and (b), the United States of America requests the issuance of a temporary restraining order, preliminary injunction, and permanent injunction against the Defendants and their agents as the Court deems just in order to prevent a continuing and substantial injury to the owners and legitimate users of the infected computers in the Coreflood Botnet.

COUNT II

(Injunctive Relief Under 18 U.S.C. § 1345)

27. The United States of America alleges and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

28. The Defendants are engaging in bank fraud, in violation of Title 18, United States, Section 1344, in that the Defendants did knowingly execute a scheme and artifice to defraud a financial institution.

29. Pursuant to Title 18, United States Code, Sections 1345(a)(1) and (b), the United States of America requests the issuance of a temporary restraining order, preliminary injunction, and permanent injunction against the Defendants and their agents as the Court deems just in order to prevent a continuing and substantial injury to the owners and legitimate users of the infected computers in the Coreflood Botnet.

COUNT III
(Injunctive Relief Under 18 U.S.C. § 2521)

30. The United States of America alleges and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

31. The Defendants are engaging in the unauthorized interception of electronic communications, in violation of Title 18, United States Code, Section 2511, in that the Defendants did intentionally intercept an electronic communication, and did intentionally use, and endeavor to use, the contents of an electronic communication, knowing that the information was obtained through the unauthorized interception of an electronic communication.

32. Pursuant to Title 18, United States Code, Section 2521, the United States of America requests the issuance of a temporary restraining order, preliminary injunction, and permanent injunction against the Defendants and their agents as the Court deems just in order to prevent a continuing and substantial injury to the owners and legitimate users of the infected computers in the Coreflood Botnet.

PRAYER FOR RELIEF

WHEREFORE the plaintiff United States of America prays that the Court issue, pursuant to Title 18, United States Code, Sections 1345(b) and 2521, a temporary restraining order, preliminary injunction, and permanent injunction against the Defendants and all those receiving notice thereof, including the Domain Service Providers, as follows:

1. A temporary restraining order and preliminary injunction that prohibits the Defendants (a) from using Coreflood to engage in wire fraud, bank fraud, or unauthorized interception of electronic communications, and (b) from running Coreflood on any computers not owned by the Defendants, by authorizing the operation of a substitute command and control server to give effect to the Court's orders;

2. A permanent injunction that requires the Defendants to uninstall Coreflood on any computers not owned by the Defendants and authorizes the operation of a substitute

command and control server to give effect to the Court's orders; and

3. Such other relief as the Court deems just and proper.

Dated: April 11, 2011
New Haven, Connecticut

Respectfully submitted,

DAVID B. FEIN
UNITED STATES ATTORNEY

By: /s/ Edward Chang
EDWARD CHANG (ct26472)
Assistant United States Attorney
157 Church St., 23rd floor
New Haven, CT 06510
Tel: (203)821-3796
Fax: (203)773-5373

/s/ David C. Nelson
DAVID C. NELSON (ct25640)
Assistant United States Attorney
450 Main St.
Hartford, CT 06103
Tel: (860)947-1101
Fax: (860)240-3291

SCHEDULE A:
The COREFLOOD DOMAINS

(1) antrexhost.com

Registry:	Verisign, Inc. 21355 Ridgetop Circle Dulles, Virginia
Registrar:	Above.com Pty Ltd 8 East Concourse, Beaumaris, VIC 3193, Australia
DNS provider:	Above.com Pty Ltd 8 East Concourse, Beaumaris, VIC 3193, Australia

(2) diplodoger.com

Registry:	Verisign, Inc. 21355 Ridgetop Circle Dulles, Virginia
Registrar:	LiquidNet Ltd. 13 Craigleith 7 Kersfield Road, Putney London SW15 3HN, United Kingdom
DNS provider:	ZoneEdit, LLC 8100 NE Parkway Drive, suite 300 Vancouver, Washington

(3) ehostville.com

Registry:	Verisign, Inc. 21355 Ridgetop Circle Dulles, Virginia
Registrar:	Network Solutions, LLC 13861 Sunrise Valley Drive, suite 300 Herndon, Virginia
DNS provider:	ZoneEdit, LLC 8100 NE Parkway Drive, suite 300 Vancouver, Washington

(4) fishbonetree.biz

Registry: Neustar, Inc.
46000 Center Oak Plaza
Sterling, Virginia

Registrar: Active Registrar, Inc.
10 Anson Road no. 16-16,
International Plaza Singapore 079903

DNS provider: Active Registrar, Inc.
10 Anson Road no. 16-16,
International Plaza Singapore 079903

(5) hostfields.net

Registry: Verisign, Inc.
21355 Ridgetop Circle
Dulles, Virginia

Registrar: Dotster, Inc.
8100 NE Parkway Drive, suite 300
Vancouver, Washington

DNS provider: ZoneEdit, LLC
8100 NE Parkway Drive, suite 300
Vancouver, Washington

(6) hostnetline.com

Registry: Verisign, Inc.
21355 Ridgetop Circle
Dulles, Virginia

Registrar: MyDomain, Inc.
8100 NE Parkway Drive, suite 300
Vancouver, Washington

DNS provider: ZoneEdit, LLC
8100 NE Parkway Drive, suite 300
Vancouver, Washington

(7) licensevalidate.net

Registry: Verisign, Inc.
21355 Ridgetop Circle
Dulles, Virginia

Registrar: Tucows Inc.
96 Mowat Avenue
Toronto, Ontario M6K 3M1 Canada

DNS provider: ZoneEdit, LLC
8100 NE Parkway Drive, suite 300
Vancouver, Washington

(8) medicalcarenews.org

Registry: Public Interest Registry
1775 Wiehle Avenue, suite 200
Reston, Virginia

Registrar: Active Registrar, Inc.
10 Anson Road no. 16-16,
International Plaza Singapore 079903

DNS provider: Active Registrar, Inc.
10 Anson Road no. 16-16,
International Plaza Singapore 079903

(9) medinnovation.org

Registry: Public Interest Registry
1775 Wiehle Avenue, suite 200
Reston, Virginia

Registrar: MyDomain, Inc.
8100 NE Parkway Drive, suite 300
Vancouver, Washington

DNS provider: ZoneEdit, LLC
8100 NE Parkway Drive, suite 300
Vancouver, Washington

(10) nethostplus.net

Registry: Verisign, Inc.
21355 Ridgetop Circle
Dulles, Virginia
Registrar: Tucows Inc.
96 Mowat Avenue
Toronto, Ontario M6K 3M1 Canada

DNS provider: Sedo.com, LLC
161 First Street, 4th floor
Cambridge, Massachusetts

(11) netwebplus.net

Registry: Verisign, Inc.
21355 Ridgetop Circle
Dulles, Virginia

Registrar: MyDomain, Inc.
8100 NE Parkway Drive, suite 300
Vancouver, Washington

DNS provider: ZoneEdit, LLC
8100 NE Parkway Drive, suite 300
Vancouver, Washington

(12) realgoday.net

Registry: Verisign, Inc.
21355 Ridgetop Circle
Dulles, Virginia

Registrar: Tucows Inc.
96 Mowat Avenue
Toronto, Ontario M6K 3M1 Canada

DNS provider: Netfirms.com - US
70 Blanchard Road, 3rd floor
Burlington, Massachusetts

(13) stafilocox.net

Registry: Verisign, Inc.
21355 Ridgetop Circle
Dulles, Virginia

Registrar: Mesh Digital Limited
3 Quarry Court Lime Quarry Mews Guildford
Surrey GU1 2RD, United Kingdom

DNS provider: Domainmonster.com, Inc.
One Broadway 14th Floor,
Kendall Square
Cambridge, Massachusetts

(14) unreadmsg.net

Registry: Verisign, Inc.
21355 Ridgetop Circle
Dulles, Virginia

Registrar: pair Networks, Inc.d/b/a pairNIC
2403 Sidney Street, suite 510
Pittsburgh, Pennsylvania

DNS provider: pair Networks, Inc.d/b/a pairNIC
2403 Sidney Street, suite 510
Pittsburgh, Pennsylvania

(15) vip-studions.net

Registry: Verisign, Inc.
21355 Ridgetop Circle
Dulles, Virginia

Registrar: Misk.com, Inc.
1542 Route 52
Fishkill, New York

DNS provider: Misk.com, Inc.
1542 Route 52
Fishkill, New York