

**UNITED STATES DISTRICT COURT
DISTRICT OF CONNECTICUT**

UNITED STATES OF AMERICA,

Plaintiff,

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,**

Defendants.

No. 3:11 CV 561 (VLB)

TEMPORARY RESTRAINING ORDER

WHEREAS the plaintiff United States of America

**("Government") has filed a complaint against the Defendants, alleging
that the Defendants are using malicious software known as
"Coreflood" to commit wire fraud and bank fraud in violation of Title
18, United States Code, Sections 1343 and 1344, and to engage in
unauthorized interception of electronic communications in violation of
Title 18, United States Code, Section 2511;**

**WHEREAS the Government has properly alleged that the
Court has subject matter jurisdiction over this action and personal**

2011 APR 12 P 1:25
US DISTRICT COURT
HARTFORD CT

FILED

jurisdiction over the Defendants, and that venue is proper in this district;

WHEREAS the Government has filed an ex parte motion for a temporary restraining order, supported by a memorandum of law and by the declaration of FBI Special Agent Kenneth Keller, seeking to enjoin the Defendants, inter alia, from running Coreflood on computers infected by Coreflood, pursuant to Title 18, United States Code, Sections 1345 & 2511 and Rule 65 of the Federal Rules of Civil Procedure;

WHEREAS the Government has shown good cause to believe: (a) that hundreds of thousands of computers are infected by Coreflood, known collectively as the "Coreflood Botnet"; (b) that the computers infected by Coreflood can be remotely controlled by the Defendants, using certain computer servers known as the "Coreflood C&C Servers" and certain Internet domains known as the "Coreflood Domains"; (c) that, on or about April 12, 2011, the Government will execute seizure warrants for the Coreflood C&C Servers and the Coreflood Domains; (d) that the Government's seizure of the Coreflood

C&C Servers and the Coreflood Domains will leave the infected computers still running Coreflood; (e) that allowing Coreflood to continue running on the infected computers will cause a continuing and substantial injury to the owners and users of the infected computers, exposing them to a loss of privacy and an increased risk of further computer intrusions; and (f) that it is feasible to stop Coreflood from running on infected computers by establishing a substitute command and control server;

WHEREAS the Coreflood Domains are listed in Schedule A, together with the corresponding registry, registrar, and domain name service ("DNS") provider (collectively, the "Domain Service Providers") used by the Defendants with respect to each of the Coreflood Domains;

WHEREAS the Government has shown good cause to believe that: (a) it is reasonably likely that the Government can show that the Defendants are committing wire fraud and bank fraud and are engaging in unauthorized interception of electronic communications, as alleged; (b) it is reasonably likely that the Government can show a

continuing and substantial injury to a class of persons, viz., the owners and users of computers infected by Coreflood; and (c) it is reasonably likely that the Government can show that the requested restraining order will prevent or ameliorate injury to that class of persons;

WHEREAS the Government has shown good cause to believe that any delay in entering this Order will cause immediate and irreparable injury, loss, or damage (a) to the Government, by preventing the Government from securing its control over the Coreflood Botnet; and (b) to the owners and legitimate users of infected computers in the Coreflood Botnet, who would suffer a continuing loss of privacy and an increased risk of further computer intrusions;

WHEREAS, having demonstrated probable cause to believe that the infected computers in the Coreflood Botnet are being used as instrumentalities of crime, the Government has further shown that there are special needs, including the need to protect the public and to perform community caretaking functions, that are beyond the normal

need for law enforcement and make the warrant and probable-cause requirement of the Fourth Amendment impracticable; and

WHEREAS the requested temporary restraining order is both minimally intrusive and reasonable under the Fourth Amendment;

NOW, THEREFORE, IT IS HEREBY ORDERED AND DECREED this 12th day of April 2011, at 9:30 a.m./~~p.m.~~:

1. The Defendants, their agents and representatives, and anyone acting under their direction or control are prohibited from using Coreflood in furtherance of any scheme to commit wire fraud or bank fraud or to engage in unauthorized interception of electronic communications and, in particular, are prohibited from running Coreflood on any computers not owned by the Defendants.
2. Pursuant to the authority granted by 28 U.S.C. § 566, the United States Marshal for the District of Connecticut ("USMS") shall execute and enforce this Order, with the assistance of the Federal Bureau of Investigation ("FBI") if needed, by establishing a substitute server at the Internet Systems Consortium, or such other Internet hosting provider as may be appropriate, that will respond to

requests addressed to the Coreflood Domains by issuing instructions that will cause the Coreflood software on infected computers to stop running, subject to the limitation that such instructions shall be issued only to computers reasonably determined to be in the United States.

3. The Defendants, their agents and representatives, and anyone acting under their direction or control, including the Domain Service Providers, shall take all measures reasonably available to them to direct Internet traffic addressed to the Coreflood Domains to the afore-mentioned substitute server. In particular:

a. Each registry or registrar of one of the Coreflood Domains receiving notice of this Order shall set the authoritative DNS name servers for that Internet domain name as follows, and shall impose a registry lock on the Internet domain name and shall lock any account associated with the registrant of the Internet domain name to prevent any change, transfer, or deletion of such Internet domain name or account:

NS1.CYBERWATCHFLOOR.COM
IP address: 204.74.66.143

NS2.CYBERWATCHFLOOR.COM
IP address: 204.74.67.143

- b. Each DNS provider for one of the Coreflood**

Domains receiving notice of this Order shall respond to DNS resolution requests for that Internet domain name by returning the IP address 149.20.51.124, or such other IP address as may be directed by FBI Special Agent Kenneth Keller, and shall lock any account associated with the Internet domain name to prevent any change, transfer, or deletion of such account.

- 4. Nothing in this Order shall permit the USMS or FBI to store, review, or otherwise use any data that may be transmitted to the substitute server from an infected computer, other than the originating IP address, network port, and the date and time of transmission.**

5. This Order shall expire on the 24th day of April 2011, at 1:30 a.m./p.m. [not to exceed 14 days], subject to the further order of this Court.

IT IS SO ORDERED.

April 12, 2011
HON. VANESSA L. BRYANT
UNITED STATES DISTRICT JUDGE

**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-studios.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