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 23, 2011
	:	
Defendants.	:	

GOVERNMENT'S SUPPLEMENTAL MEMORANDUM
IN SUPPORT OF PRELIMINARY INJUNCTION

The Government respectfully submits this supplemental memorandum in support of its motion for a preliminary injunction. This supplemental memorandum describes: (1) the implementation and effect of the temporary restraining order ("TRO") issued by the Court; (2) the status of the Government's efforts to notify Coreflood victims; (3) the steps that have been taken to serve process on the Defendants; and (4) the reasons why the relief granted in the TRO should be continued as a preliminary injunction.

For the reasons set forth herein, and in the Government's Memorandum of Law in Support of Motion for Temporary Restraining Order, Preliminary Injunction, and Other Ancillary Relief, dated Apr. 12, 2011 [Dkt No. 32] ("Gov't Memo."), the Government respectfully requests the entry of a preliminary injunction to last for thirty days, until May 25, 2011 or such other date as may be convenient to the Court to conduct a hearing on the final disposition of this matter.

Background

A. The Implementation and Effect of the TRO

On April 12, 2011, the Government seized five Coreflood C&C Servers and numerous Coreflood Domains, pursuant to search warrants and a seizure warrant, respectively. See Declaration of Briana Neumiller, dated Apr. 23, 2011 ("Neumiller Decl."), ¶ 3. The Government also put into operation two substitute servers,[*] as authorized by the Court, for the purpose of responding to command and control requests from infected computers by directing Coreflood to stop running. See Temporary Restraining Order, dated Apr. 12, 2011

[*] The second substitute server was taken out of operation on April 21. See Neumiller Decl. ¶ 4.

[Dkt No. 10]; Supplemental Order, dated Apr. 12, 2011 [Dkt No. 27]; Supplemental Temporary Restraining Order, dated Apr. 12, 2011 [Dkt No. 41]. Later, in response to a request for law enforcement assistance from the United States, authorities in Estonia seized several additional computer servers, believed to be "predecessors" of the Coreflood C&C servers seized in the United States. See Neumiller Decl. ¶ 3; see also Complaint ¶ 3 (defining "predecessors" of a C&C server).

The coordinated seizures and the TRO have had the following effects: (1) they have temporarily stopped Coreflood from running on infected computers in the United States, thereby preventing further loss of privacy and damage to the financial security of owners and users of the infected computers; and (2) they have stopped Coreflood from updating itself, thereby enabling anti-virus software vendors to release new virus signatures that can recognize the latest versions of Coreflood.

As shown in Figure 1, the size of the Coreflood Botnet has been diminishing steadily, based on the number of beacons per day

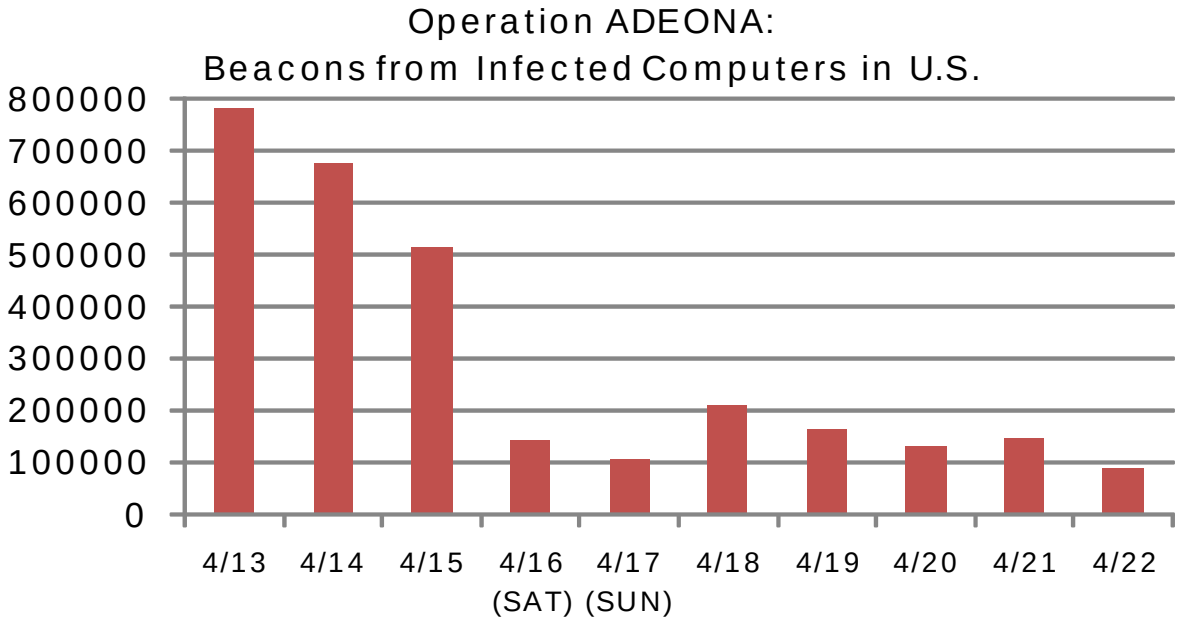

Figure 1: Coreflood Beacons per Day

sent by infected computers to the substitute servers.* See Neumiller Decl. ¶ 4. Figure 1 shows only the beacons per day originating from infected computers within the United States, inasmuch as the

* While the beacons per day ("BPD") metric is a reasonable measure of the size of the Coreflood Botnet, it is not the same as the number of infected computers because an infected computer may be re-started several times per day (increasing the BPD) or not re-started or turned on at all (decreasing the BPD). The actual number of infected computers in the Coreflood Botnet is not known, notwithstanding the Government's control of the substitute servers, because the Government is not receiving content from the infected computers, including content that would enable the Government to uniquely identify each infected computer.

substitute servers have been responding only to infected computers within the United States in accordance with the TRO.

The Coreflood Botnet is believed to be diminishing in size for two reasons. See id. ¶ 6. First, because Coreflood has not been able to update itself on infected computers, anti-virus vendors are no longer faced with a moving target and have been able to release virus signatures capable of detecting the latest versions of Coreflood. See id. Second, as victims of Coreflood are notified of their infected computers, they may be disconnecting the infected computers from the Internet or taking other measures to remediate Coreflood. See id.

Additional time is needed, however, both to allow more anti-virus vendors to release virus signatures for Coreflood and to complete the process of notifying Coreflood victims.

B. Notification of Coreflood Victims

After seizing control of the Coreflood Botnet, the FBI New Haven field office ("FBI/NHFO") began the task of notifying the owners of hundreds of thousands of infected computers. As indicated previously, the primary mechanism for notifying Coreflood victims has

been to provide Internet service providers ("ISPs") with the IP addresses of their customers who are infected with Coreflood. See Gov't Memo. at 25. Each ISP was also provided with a form Notice of Infected Computer and asked to provide copies of the notice or its equivalent to infected customers. See Neumiller Decl. ¶ 8 & Ex. A. The Government has been advised that several ISPs have already begun the process of notifying their affected customers. See id.

In certain cases, publicly available records on the Internet can be used to match IP addresses of infected computers to entities with known IP addresses (the "Identifiable Victims"). See id. ¶¶ 7 & 9. The Identifiable Victims to date include approximately seventeen state or local government agencies, including one police department; three airports; two defense contractors; five banks or financial institutions; approximately thirty colleges or universities; approximately twenty hospital or health care companies; and hundreds of businesses. See id. ¶ 9. The FBI/NHFO has distributed information about the Identifiable Victims to the pertinent FBI field offices, which have

begun notifying the Identifiable Victims in their geographic regions. See id.

In addition to providing each Identifiable Victim with the form Notice of Infected Computer, the FBI is also providing a form Authorization to Delete Coreflood from Infected Computer(s). See id. ¶ 9 & Ex. B. This authorization form allows an Identifiable Victim to request and consent to the removal of Coreflood from infected computers, as described more fully below.

Finally, the FBI/NHFO has provided the IP addresses of foreign computers infected with Coreflood, sorted by country, to the FBI International Operations Division. Those IP addresses are being distributed, as appropriate, by FBI legal attachés to foreign law enforcement authorities. See id. ¶ 10.

C. Service of Process on the Defendants

The Defendants have been served in accordance with the Court's Order Authorizing Service, dated Apr. 12, 2011 [Dkt No. 12]. Specifically, on April 13, the following documents were sent by electronic mail to the last-known email address of each Defendant:

the Complaint, the TRO, the Supplemental TRO, the Order to Show Cause, and the Forfeiture Warrant. See Declaration of Jane Domboski, dated Apr. 23, 2011 ("Domboski Decl.") ¶ 4. The summons for each Defendant was served by electronic mail on April 15, 2011. See id. ¶ 5. Copies of all of the documents were mailed by Federal Express to the last-known address* of each Defendant on April 20, 2011. See id. ¶ 6. Finally, all of the documents have also been posted on the publicly available Internet sites of the FBI/NHFO and the United States Attorney's Office. See id. ¶¶ 4 & 7.

In addition to the formal methods of service of process, the Defendants are likely to have received notice of this action through the extensive media coverage it has received. Soon after the case was unsealed, Internet sites including Yahoo!, CNN, ABC News, Information Week, and Wired all reported on the seizures and on the Court's issuance of a TRO to stop Coreflood from running on infected computers. See id. ¶ 8. There was also international news coverage,

---

* Physical mailings were not sent to Defendants whose addresses were known to be false or fraudulent. See Domboski Decl. ¶ 6.

for example, on the Internet sites of the International Business Times and the Moscow Times. See id.

In sum, the Defendants have been properly served in this action, and are likely to have received actual notice of this action as well.

D. Need for Continuing Equitable Relief

As shown previously in Figure 1, the Coreflood Botnet is gradually diminishing in size. The Government believes that the equitable relief provided in the TRO has proven effective, but that there is an ongoing need to prevent a continuing and substantial injury to the owners and users of computers still infected by Coreflood. In particular, the TRO is only temporarily stopping Coreflood from running on infected computers, because Coreflood attempts to run whenever an infected computer is turned on or re-started. See Gov't Memo. at 24-25. Therefore, without continuing equitable relief: (1) the computers still infected with Coreflood will be running a malicious program that the owners and users do not know about and never intended to have running; (2) the program will continue to put at risk

the privacy and confidentiality of Internet communications, including private personal and financial information; and (3) the program could enable computers still infected with Coreflood to be used in furtherance of other criminal activity, if the Defendants or others with criminal intent were to re-establish control over them. See Gov't Memo. at 42-43.

The effectiveness of the equitable relief may be seen by comparing the rate of decline of Coreflood-infected computers in the United States with Coreflood-infected computers in foreign countries, as shown in Figure 2. See Neumiller Decl. ¶ 5. Because infected computers in foreign countries are not receiving instructions to stop running Coreflood, and are therefore beaconing more frequently to the substitute servers than infected computers in the United States, the data in Figure 2 has been normalized by using the number of beacons per day on April 13, 2011 as a reference point. See id. Figure 2 shows that the size of the Coreflood Botnet has been reduced by nearly 90%

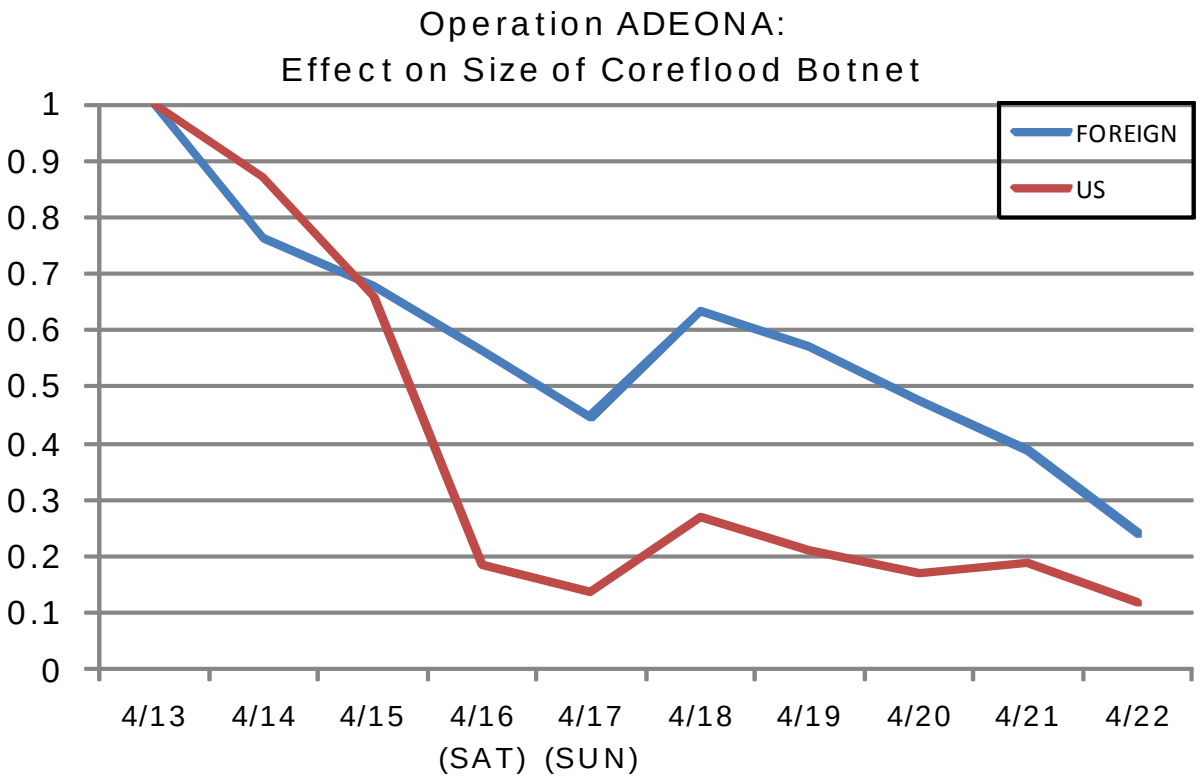

Figure 2: Normalized Beacons per Day

in the United States and more than 75% overseas.

While it is not known with certainty why Coreflood is being remediated more quickly in the United States than overseas, two known differences are that (1) the TRO was only enforced within the United States, and (2) the FBI's victim notification efforts have already reached numerous victims in the United States, but have likely not yet reached as many victims overseas.

Moreover, there is anecdotal evidence that the equitable relief in the TRO has been of considerable value to the victims. In one example, the chief information security officer of a hospital healthcare network reported that, after being notified by the FBI of a Coreflood infection, a preliminary investigation revealed that approximately 2,000 of the hospital's 14,000 computers were infected by Coreflood. Because Coreflood was no longer running on the infected computers (as a result of the TRO and the operation of the substitute servers), the hospital was able to focus on investigating and repairing the damage instead of scrambling to stanch the loss of data from thousands of infected computers. See id. ¶ 11.

Under the circumstances, the Government respectfully submits that the equitable relief in the TRO should be continued as a preliminary injunction.

While the proposed preliminary injunction is in effect, the Government also expects to uninstall Coreflood from the computers of Identifiable Victims who provide written consent. The Government is not requesting explicit authorization from the Court to do so, because

the written consent form obviates the need for such authorization. Nevertheless, in order to keep the Court fully apprised of all relevant facts, the Government respectfully advises the Court that the substitute server, or another similar server, will be configured to respond to command and control requests from infected computers by issuing instructions for Coreflood to uninstall itself, but only as to infected computers of Identifiable Victims who have provided written consent to do so. See id. ¶ 12.

While the use of an "uninstall" command to remove Coreflood cannot be considered a replacement for the use of properly configured and updated anti-virus software, removing Coreflood from infected computers will at least serve to eliminate a known threat to that victim's privacy and financial security.

ARGUMENT

The Court may decide the Government's motion for a preliminary injunction on the papers if "the relevant facts either are not in dispute . . . or when the disputed facts are amenable to complete resolution on a paper record." Charette v. Town of Oyster Bay, 159 F.3d 749, 755 (2d Cir. 1998).

In this case, the Defendants have been properly served, and despite the considerable publicity accompanying this case, they have not appeared to dispute the issuance of a TRO or any of the facts contained in the sworn declarations submitted by the Government in support of the TRO. Accordingly, the declarations are sufficient to carry the Government's burden of proof. See, e.g., Cartier, A Div. of Richemont N. Am., Inc. v. Aaron Faber Inc., 382 F. Supp. 2d 625, 625 (S.D.N.Y. 2005) (granting preliminary injunction where defendants failed to respond to order to show cause); see also The Ernest Lawrence Group, Inc. v. Government Careers Ctr. of Oakland, Calif., No. 99 Civ. 3807 (DC), 2000 WL 1655234, at *1 (S.D.N.Y. Nov. 3, 2000).

In particular, the equitable relief granted in the TRO has been effective in preventing Coreflood from causing continuing and substantial injury to the owners and users of infected computers. It has also been effective in reducing the size of the Coreflood Botnet itself, by allowing anti-virus vendors to release updated virus signatures and by giving the Government an opportunity to notify victims of infected computers.

In sum, the Government respectfully submits that the TRO should be continued as a preliminary injunction, to prevent a continuing and substantial injury to owners of computers still infected by Coreflood and to provide sufficient time for victims of Coreflood to receive notice and to take action to protect themselves.

Conclusion

The Government's motion for a preliminary injunction should be granted.

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