IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	
	)	
Plaintiff,	)	Civil Action No.
	)	
v.	)	**FILED *EX PARTE***
	)	**AND UNDER SEAL**
"flux"	)	
a/k/a "ffhost,"	)	
	)	
and,	)	
	)	
"flux2"	)	
a/k/a "ffhost2"	)	
	)	
Defendants.	)	

COMPLAINT

Plaintiff, the United States of America, by and through its undersigned counsel, alleges the following:

1. This is a civil action brought under Title 18, United States Code, Sections 1345 and 2521 and Federal Rule of Civil Procedure 65, to enjoin 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 providing an unattributable digital infrastructure of interconnected computers, known as "Avalanche," through which Defendants and their accomplices communicate with armies of malware-infected computers or communicate with their money mules who are moving large sums of money stolen from victims all over the world.

2. Defendants advertise Avalanche in known criminal forums as a fast fluxing bullet-proof hosting service. The Defendants, through the Avalanche infrastructure, have knowingly

hosted at least 16 malware campaigns and numerous money mule rings with victims around the world including in the United States and the Western District of Pennsylvania.

3. Among the malware being hosted by Defendants and their accomplices through the Avalanche infrastructure is Nymaim. Nymaim is a malware that, among other things, encrypts files on a victim's computer until the victim pays a ransom for a key to decrypt their own files. A feature of the Nymaim malware is an included keystroke logger which captures every keystroke made on a victim's infected computer and transfers the keystrokes back through the Avalanche infrastructure. In January 2015, a state governmental entity in Allegheny County in the Western District of Pennsylvania fell prey to the Nymaim malware which used the Avalanche network to communicate with the conspirators. The latest version of Nymaim is Goznym.

4. In February through April, 2016, a company in New Castle, Pennsylvania in the Western District of Pennsylvania, suffered seven attempted wire transfers of funds from their bank account totaling over $240,000. The New Castle company's infected computer was examined and found to be infected with the Goznym malware. No other malware variant was found.

5. In April 2016, a company located in Carnegie, Pennsylvania in the Western District of Pennsylvania suffered an attempted fraudulent wire transaction for $387,500 had been initiated from the company's online account through a Pittsburgh financial institution to a bank account in Bulgaria. A subsequent analysis of the infected Carnegie company computer revealed the Goznym malware infected the computer. No other malware variant was found on the computer.

6. Another malware that Defendants deploy through Avalanche is Corebot. Corebot is a Trojan with a focus on stealing banking and credential information for accessing online bank accounts. Corebot utilizes several features including browser-based web injects which present a malicious webpage to a victim which mimics a legitimate bank website to intercept log in credentials of the victim to be used instead by Defendants and their accomplices to steal the victims' funds from their bank accounts. A number of computers in the Western District of Pennsylvania are infected with this malware.

7. Once a victim's computer is infected with the various malware, it becomes a "bot" in one or more of the many botnets that are controlled by Defendants and their accomplices. Defendants' Avalanche infrastructure is used to communicate instructions to these bots as well as to receive stolen information from the compromised victim computers. It is estimated that over 1 million computers have been infected with malware that is run through the Avalanche infrastructure since Avalanche was first started sometime around 2010. The infected machines are located all over the world, including a significant number in the United States and the Western District of Pennsylvania.

8. Defendants hide the communications between the bots and the botmasters through Avalanche's complicated structure of tiered proxy servers with quickly changing domains and IP addresses which pass the communications to and from the command and control (C&C) servers accessed by Defendants and their accomplices.

Parties

9. Plaintiff is the United States of America.

10. Defendants "flux" and "flux2" are only currently known by their online monikers.

Jurisdiction and Venue

11. Subject matter jurisdiction lies pursuant to Title 18, United States Code, Sections 1345(a)(1) and 2521 and Title 28, United States Code, Sections 1331 and 1345.

12. The defendants are subject to the personal jurisdiction of this Court, having conspired to infect computers, used infected computers in furtherance of their scheme to defraud, initiated fraudulent money transfers, and engaged in unauthorized wiretapping, within the Western District of Pennsylvania.

13. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2).

The Avalanche Scheme to Defraud and Unauthorized Interception

14. A botnet is a collection of compromised computers that are controlled, without the knowledge of the victims, by an unauthorized third party. A botnet can be used for many criminal purposes, including sending spam, stealing data, and committing financial fraud.

15. The botnets being hosted by Defendants on the Avalanche infrastructure are used for the commission of fraudulent financial activity. For example, the principal purpose of Corebot is to capture banking credentials from infected computers. One means by which Corebot accomplishes this is through "man-in-the-middle" attacks, in which Corebot intercepts sensitive information victims transmit from their computers.

16. To increase the effectiveness of such attacks, the defendants use Corebot to inject additional code into victims' web browsers that changes the appearance of the websites victims

are viewing. For example, if a Corebot-infected user were to visit a banking website that typically requests only a username and password, the defendants could seamlessly inject additional form fields into the website displayed in the user's web browser that also request the user's social security number, credit card numbers, and other sensitive information. Because these additional fields appear to be part of the legitimate website users elected to visit, users are often defrauded into supplying the requested information, which is promptly intercepted by Corebot and transmitted to the Defendants and their accomplices through the Avalanche infrastructure.

17. Victims of the Defendant's scheme to defraud and unauthorized interception include, among others:

a. A state governmental entity in Allegheny County in the Western District of Pennsylvania;
b. A company in New Castle, Pennsylvania; and,
c. A company in Carnegie, Pennsylvania.

18. Since Avalanche first emerged in 2010, total losses attributable to Avalanche are estimated to be in the hundreds of million dollars worldwide.

COUNT I
(Injunctive Relief under 18 U.S.C. § 1345)

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

20. The Defendants are engaging in conspiracy to commit wire fraud, in violation of Title 18, United States Code, Sections 1343 and 1349, in that the defendants, having devised a scheme or artifice to defraud and for obtaining money by means of false or fraudulent pretenses, are transmitting and causing 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.

21. Pursuant to Title 18, United States Code, Section 1345(a) 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 in order to prevent a continuing and substantial injury to the owners and legitimate users of the infected computers using Avalanche to communicate with the perpetrators.

COUNT II
(Injunctive Relief under 18 U.S.C. § 1345)

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

23. The Defendants are engaging in conspiracy to commit bank fraud, in violation of Title 18, United States Code, Sections 1344 and 1349, in that the defendants are knowingly executing a scheme or artifice to defraud financial institutions insured by the Federal Deposit Insurance Corporation and to obtain moneys under the custody and control of these institutions by means of false and fraudulent pretenses and representations.

24. Pursuant to Title 18, United States Code, Section 1345(a) 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 accomplices and agents in order to prevent a continuing and substantial injury to the owners and legitimate users of the infected computers using Avalanche to communicate with the perpetrators.

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

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

26. 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 are conspiring to intentionally intercept electronic communications, and are conspiring to intentionally use and endeavor to use the contents of electronic communications knowing that the information is obtained through the unauthorized interception of electronic communications.

27. 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 accomplices and agents in order to prevent a continuing and substantial injury to the owners and legitimate users of the infected computers using Avalanche to communicate with the perpetrators.

PRAYER FOR RELIEF

WHEREFORE, the United States of America prays that the Court:

A. Enter judgment in favor of the Government and against the Defendants;

B. Pursuant to Title 18, United States Code, Sections 1345(b) and 2521, enter a preliminary injunction and a permanent injunction against the Defendants and their agents, servants, employees, and all persons and entities in active concert or participation with them from engaging in any of the activity complained of herein or from causing any of the injury

complained of herein and from assisting, aiding or abetting any other person or business entity from engaging in or performing any of the activity complained of herein or from causing any of the injury complained of herein;

C. Pursuant to Title 18, United States Code, Sections 1345(b) and 2521, enter a preliminary injunction and permanent injunction authorizing the Government to continue the malware disruption plan specified in the Government's Memorandum of Law in Support of Motion for Temporary Restraining Order, Order to Show Cause, and Other Ancillary Relief for a period of six months, and requiring the entities specified in the Temporary Restraining Order to continue take the actions specified in the Temporary Restraining Order for a period of sixty days.

D. Order such other relief that the Court deems just and proper.

Respectfully submitted,

DAVID J. HICKTON
United States Attorney

By: /s/ Michael A. Comber
MICHAEL COMBER
Assistant U.S. Attorney
Western District of PA
U.S. Post Office & Courthouse
700 Grant Street, Suite 4000
Pittsburgh, PA 15219
(412) 894-7485 Phone
(412) 644-6995 Fax
PA ID No. 81951
Michael.Comber@usdoj.gov

LESLIE R. CALDWELL
Assistant Attorney General

By: /s/ Richard D. Green
RICHARD D. GREEN
Senior Trial Attorney
Computer Crime and Intellectual Property Section
1301 New York Avenue NW
Washington, DC 20530
(202) 514-1026 Phone
(202) 514-6113 Fax
PA Bar No. 43758
Richard.Green@usdoj.gov