RECEIVED
NOV 28 2016
CLERK, U.S. DISTRICT COURT
WEST. DIST. OF PENNSYLVANIA

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.	)	

UNITED STATES' MEMORANDUM OF LAW IN SUPPORT OF MOTION FOR TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

Plaintiff, the United States of America, by and through its attorneys, David J. Hickton, United States Attorney for the Western District of Pennsylvania, Leslie R. Caldwell, Assistant Attorney General, Michael A. Comber, Assistant United States Attorney, and Richard D. Green, Senior Trial Attorney, pursuant to 18 U.S.C. §§ 1345, 2521, and Federal Rule of Civil Procedure 65, hereby seeks an *ex parte* temporary restraining order commanding the defendants to halt a massive fraud and wiretapping scheme that is harming consumers, financial institutions, and other businesses in the United States and around the world.

I. OVERVIEW

The defendants in this case administer a hosting infrastructure known as "Avalanche" comprised of a worldwide network of servers controlled by through a highly organized central

control system. The Avalanche administrators rent out access to the Avalanche network to cyber criminals for the bulletproof hosting services over which the malware attacks and money mule campaigns victimize hundreds of thousands of people throughout the world.

In this action, the United States seeks injunctive relief commanding the defendants to stop using Avalanche to defraud and wiretap American citizens and businesses. To give effect to this prohibition, the United States seeks permission to employ a series of technical measures designed to disrupt the defendants' infrastructure and related malware systems. Specifically, the United States seeks an Order: (1) directing certain U.S. Domain Registries to redirect proscribed a list of domain names used by Avalanche or the malware systems that traverse it to substitute servers and, at the registries' discretion, transfer the domain names to the Registry of Last Resort (RoLR); (2) directing certain U.S. Domain Registries to cause a separate list of domain names to block access to a proscribed list of domain names used by Avalanche or the malware systems that traverse it and, at the registries' discretion, to register those with the Registry of Last Resort (RoLR); (3) directing certain U.S. Domain Registries to register a proscribed list of domain names, direct them to substitute servers, and, at the registries' discretion, transfer the domain names to the Registry of Last Resort (RoLR); and (4) directing certain U.S. Domain Registries to transfer a proscribed list of domain names and redirect them to substitute servers.

In addition to the civil relief sought above, the Government has also applied for a Pen Register/Trap and Trace Order that would authorize the collection of the dialing, routing, addressing, and signaling information of communications sent by the computers infected with Avalanche or the malware systems that traverse it to the substitute servers and other computer infrastructure established pursuant to the TRO sought by the Government. This information

would be disseminated to the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT), the ShadowServer Foundation, the Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE) that would facilitate the notification of Avalanche victims and provide instruction on how to remove these infections from their computers.[1]

This action is the latest in a string of cases brought by public and private sector entities to combat malicious software, and it is very similar to the successful Coreflood botnet disruption, which was initiated in the District of Connecticut in April 2011 ("Coreflood") and the successful botnet mitigation efforts in GameOver Zeus ("GOZ") and Dridex/Bugat ("Dridex") here in this District. *See United States v. John Doe 1 et al.*, No. 3:11-CV-00561 (D. Conn., filed Apr. 11, 2011) (Coreflood), *United States v. Bogachev*, No. 2:14-CV-0685 (W.D. Pa., filed May 26, 2014) (GOZ), *United States v. Ghinkul, et al.*, No. 2:15-CV-1315 (W.D. Pa., filed October 8, 2015) (Dridex). Coreflood, GOZ, and Dridex, like many of the malware systems that traverse Avalanche, were botnets used by criminals to intercept financial information, including login credentials, and to execute fraudulent transactions. To disable Coreflood, GOZ, and Dridex, the United States used the same authorities invoked here to deny the operators of Coreflood, GOZ, and Dridex access to the infrastructure necessary to control the botnet. In both Coreflood, GOZ, and Dridex, the Government also received judicial authorization to establish a substitute server to

[1] US-CERT is part of the Department of Homeland Security, and leads efforts to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation while protecting the constitutional rights of Americans. *See* http://www.us-cert.gov/about-us. The ShadowServer Foundation is a non-profit security research organization in the Netherlands that frequently hosts servers used in botnet remediation and has strong relationships with U.S. Internet Service Providers (ISPs). FKIE is a research organization in Bonn, Germany that provides cyber-security expertise services to German civil authorities.

replace the command and control infrastructure operated by the Coreflood, GOZ, and Dridex defendants. These actions successfully crippled the botnets and disabled the criminal enterprises.

In the years since Coreflood, the Microsoft Corporation has brought a number of civil actions against botnet operators. *See* Microsoft civil cases cited *infra* at Section VI(B). In each of these cases, Microsoft has been awarded injunctive relief – similar to the relief sought here – designed to disrupt the criminals' control over the botnet and liberate the infected computers.

The criminal enterprise responsible for Avalanche and the malware systems that traverse it has caused significant injury in this District, in the United States, and around the world. To disrupt this criminal enterprise, and to protect American citizens and businesses from falling victim to Avalanche and the malware systems that traverse it, the United States respectfully requests that this Court enter the proposed temporary restraining order ("TRO") and order the defendants to show cause why a preliminary injunction should not be granted.

II. BACKGROUND ON AVALANCHE

Avalanche is a hosting infrastructure that is composed of a worldwide network of servers that is controlled via a highly organized central control system. *See* Declaration of Special Agent Aaron Francis ("Francis Decl.") at ¶4. The Avalanche administrators rent out access to the network to other cyber criminals interested in acquiring bulletproof hosting services over which the criminals conduct malware attacks and operate money mule campaigns to launder the illegal proceeds. *Id.*

Searches and Title III interceptions conducted by the FBI confirmed that the criminal organization that controls the Avalanche infrastructure offers two general types of services to its cyber-criminal customers: (1) the registering of domain names; and (2) the redirecting (or

"proxying") of traffic through the secure Avalanche network/infrastructure to the cyber criminals who run both malware and money mule campaigns. *Id.* at ¶ 5. To further avoid detection, the administrators of Avalanche combine their two basic services with a technique known as "fast-fluxing." The basic idea behind fast fluxing is to have numerous IP addresses associated with a single domain name, where the IP addresses are swapped in and out with extremely high frequency, through changing DNS records. *Id.* at ¶ 9. The purpose of this fluxing is to thwart detection of malicious domains and IP addresses by law enforcement. *Id.*

Avalanche is remarkable for both the volume and variation of malware and money mule operations funneled through its servers. *Id.* at ¶ 10. German authorities estimate that over one million victims have been infected with malware run through the Avalanche infrastructure since this scheme began. *Id.* Avalanche has also proved to be extremely resilient to counter measures because of the frequency with which the servers in its infrastructure are changed and the measures Malware Actors and Administrators take to conceal their identity. *Id.* Moreover, the servers used in Avalanche are often paid for through stolen funds or by other means designed to thwart detection by law enforcement. *Id.*

III. THE DEFENDANTS

A multi-year FBI investigation has revealed that the defendants, who are the administrators of Avalanche, go by the monikers Flux and Flux2. *Id.* at ¶ 53. The investigation utilized search warrants and Title III wiretaps to uncover a web of communications from Flux and Flux2, to include a buddy list of more than one hundred Jabber accounts of customers

authorized to communicate over the serves with Flux and Flux2.[2] *Id.* The customers of administrators Flux and Flux2 operate the malware and money mule schemes run over the Avalanche infrastructure. *Id.* Although the full scope of harm caused by the defendants is impossible to calculate, the best evidence available suggests that Avalanche and the malware systems that traverse it have resulted in losses to U.S. businesses and individuals of more than $__ million with the true number possibly many times higher. *Id.* at ¶__.

These administrators were first identified through advertisements placed on various criminal forums. *Id.* at ¶ 54. By way of example, on November 10, 2014, a post made to the criminal forum Verified by "User41" advertised a fast fluxing bullet proof hosting service. The advertisement instructed potential customers to contact the administrators at flux@jabber-im.net and flux2@jabber-im.net. Thereafter, on October 12, 2015, a post made to the criminal forum Mazafaka by "Firestarter" advertised a fast fluxing bullet-proof hosting service. The advertisement instructed potential customers to contact the administrators at ffhost@jabber-br.org and ffhost2@jabber-br.org. In later posts by the same user these jabber contacts were changed to ffhost@xmpps.net and ffhost2@xmpps.net. Likewise, on March 24, 2016, another post made to Verified by "User41" advertised a fast fluxing bullet proof hosting service. The advertisement again instructed potential customers to contact the administrators at flux@jabber-im.net and flux2@jabber-im.net. These and other advertisements connected specific jabber contacts with the administrators of Avalanche. *Id.*

[2] Registration lists discovered during these searches revealed a set of registered domains that were used during Zeus v1 campaigns. Francis Decl. ¶ 51. The earlier versions of the Zeus variant constitute the basis to relate this matter to the GameOver Zeus matter. *See, United States v. Bogachev*, No. 2:14-CV-0685 (W.D. Pa., filed May 26, 2014).

The court authorized Title III intercepts of the administrators' private jabber provided further insight. *Id.* at ¶ 55. On April 25, 2016, support@jabbim.cz wrote to flux@jabber-im.net, "I need a VPS." Flux@jabber-im.net responded, "for what purpose is this required?" support@jabbim.cz stated, "for a botnet." *Id.* at ¶ 56. As described by Special Agent Francis, support@jabbim.cz is requesting Flux provide hosting services in order to run a botnet over the Avalanche Infrastructure. *Id.* at ¶ 57. Flux, as an administrator of the Infrastructure, is asking why the VPS is needed so he can provide the appropriate service for the customer. *Id.* Thereafter, on May 5, 2016, ffhost2@xmpps.net wrote to maestr0@xmpp.jp, "we can suggest a fastflux – redirection of traffic to your server (the abuse of service complaints remain with us. You get your usual legal server and we proxy the traffic there). *Id.* at ¶ 58. The cost is 150 a week or 450 for 4 weeks. Upon payment we immediately fend off your abuse of service complaints." *Id.* As described by Special Agent Francis, Ffhost2 is describing the Avalanche hosting service to a potential customer. *Id.* at ¶ 59. Ffhost2 further advised the customer that use of this service will cost $150 for a week or $450 for four weeks. *Id.* Further, on May 11, 2016, flux2@jabber-im.net wrote to chop@none.su, "Today is the deadline for hosting payment. If possible pay in Paymer. We would appreciate is ---- [WebMoney Account Number]." *Id.* at ¶ 60. As described by Special Agent Francis, Flux2 is advising Avalanche customer chop that his bill is due. *Id.* at ¶ 61. Flux2 further asks chop to use Paymer a form of online currency) and send the funds to WebMoney account [number]. *Id.* This particular WebMoney account received all Avalanche customer payments. *Id.*

Accordingly, the individual using the jabber accounts flux@jabber-im.net and ffhost@xmpps.net utilized these accounts to administer the Avalanche service for the

administration of the Avalanche Infrastructure. *Id.* at ¶ 63. Likewise, Flux2 aka ffhost2, using the jabber accounts flux2@jabber-im.net and ffhost2@xmpps.net, utilized these accounts to administer the Avalanche service for the administration of the Avalanche Infrastructure. *Id.*

IV. AVALANCHE AND THE MALWARE SYSTEMS THAT TRAVERSE IT HAVE HARMED AND ATTEMPTED TO HARM VICTIMS IN THIS DISTRICT

Avalanche and the malware systems that traverse it have also caused and attempted to cause significant financial losses to business operating in this District. *Id.* at ¶ 69. The data collected by the FBI and German authorities suggested that there were many victims worldwide, including in the Western District of Pennsylvania. *Id.* Although it is impossible to fully quantify the losses caused by malicious programs that traverse Avalanche, the paragraphs below provide the court with an overview of the injury in this District alone.

- From January 7-22, 2015, the servers of a state governmental entity in Allegheny County became infected by Nymaim malware. Nymamim, among other things, encrypts a victim's files until the victim pays a ransom to the perpetrator. The governmental entity paid a ransom of six Bitcoin – roughly $1,400 – in exchange for a decryption tool that decrypted its files. *Id.* at ¶ 72.

- From February – April, 2016, a company in New Castle, Pennsylvania was victimized through multiple Account Takeover (ATO) frauds that resulted in seven unauthorized wire transfers totaling $243,132.08. Following a forensic imaging of the victim's infected computer, the GozNym malware was located and identified. The unauthorized wire transactions were stopped before any money was lost. *Id.* at ¶¶ 74-77.

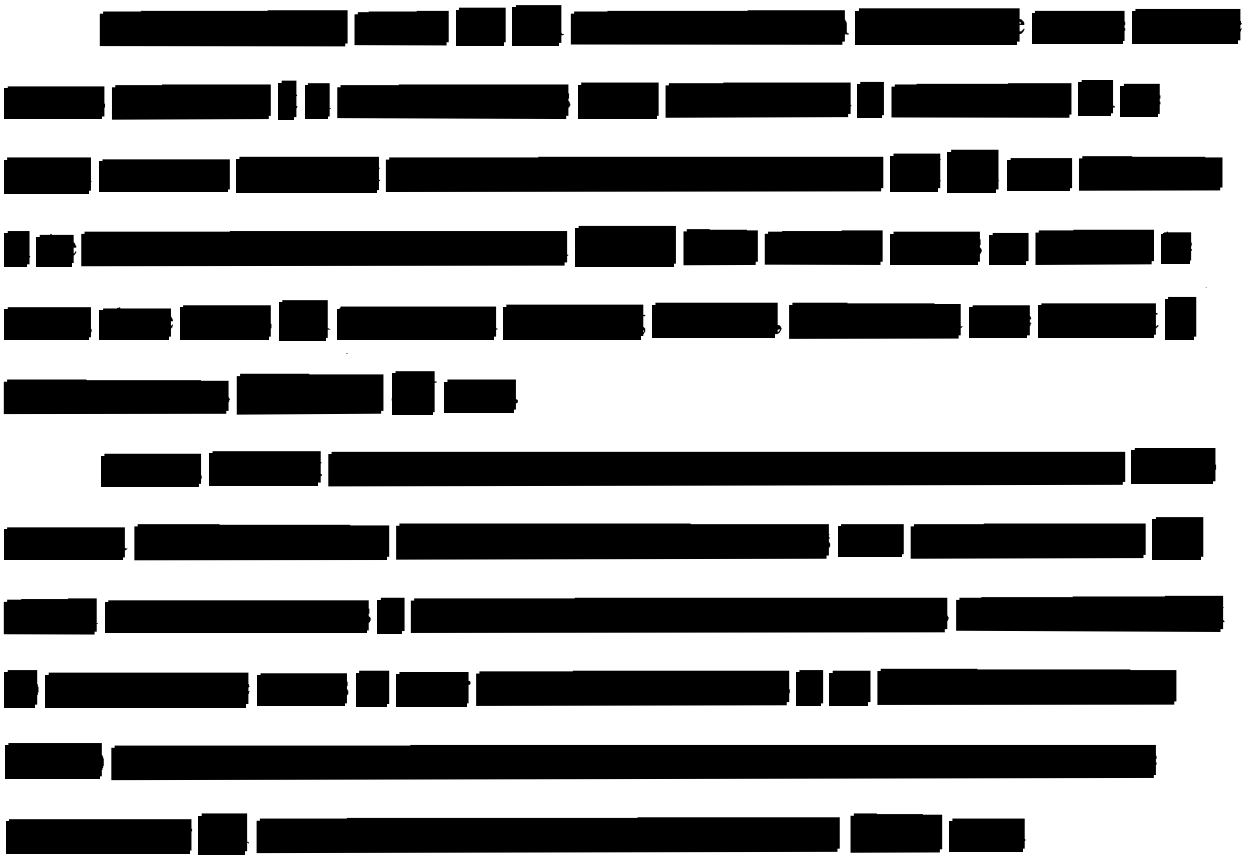
- From April 7 – 11, 2016, a company headquartered in Carnegie, Pennsylvania was also the victim of an ATO fraud that resulted in the issuance of a fraudulent wire transfer in the amount of $387,500 from a Pittsburgh-based financial institution to a Bulgarian bank account. Following a forensic imaging of the victim's infected

computer, the GozNym malware was located and identified. The unauthorized wire transactions were stopped before any money was lost. *Id.* at ¶¶ 78-79.

V. THE UNITED STATES IS PREPARED TO DISRUPT THE AVALANCHE AND THE MALWARE SYSTEMS THAT TRAVERSE IT

The FBI and German authorities have developed a comprehensive technical plan to disrupt Avalanche and the malware systems that traverse it. *Id.* at ¶ 83. A review of the technical disruption effort and subsequent remediation campaign is provided below.

[START REQUESTED REDACTION #1 OF 1]



[redacted]

[redacted]

[END REQUESTED REDACTION #1 OF 1]

VI. ARGUMENT

A. Jurisdiction and Venue Are Proper in This Court

Sections 1345 and 2521 of Title 18 authorize the United States to "commence a civil action in any Federal court" to enjoin fraud, and to "initiate a civil action in a district court of the United States" to enjoin illegal interception of communications. As detailed above, and in the Complaint filed herewith, the defendants are engaged in fraud and wiretapping against U.S. citizens and businesses on a massive scale. Accordingly, subject matter jurisdiction is proper in this Court. This Court may also exercise personal jurisdiction over the defendants, who are foreign nationals that have deliberately targeted victims in this District. Venue is proper under 28 U.S.C. § 1391(b)(2), for the reasons discussed below in relation to personal jurisdiction.

1. The Defendants Are Subject to Personal Jurisdiction in This Court Because They Have Defrauded and Engaged in Unauthorized Wiretapping of Victims in this District

At the complaint stage, a *prima facie* case by the plaintiff of personal jurisdiction is sufficient. *Eurofins Pharma US Holdings v. BioAlliance Pharma SA*, 623 F.3d 147, 155 (3d Cir. 2010). For claims arising under federal law, serving a summons or filing a waiver of service establishes personal jurisdiction over a defendant who is subject to the jurisdiction of a court of

[redacted]

general jurisdiction in the state where the district court is located. Fed. R. Civ. P. 4(k)(1); *see Provident Nat'l Bank v. California Federal Sav. & Loan Ass'n*, 819 F.2d 434, 437 (3d Cir.1987) ("A federal district court may assert personal jurisdiction over a nonresident of the state in which the court sits to the extent authorized by the law of that state."). Pennsylvania law provides for jurisdiction "to the fullest extent allowed under the Constitution of the United States" and "based on the most minimum contact with [the] Commonwealth allowed under the Constitution of the United States." 42 Pa. Cons.Stat. Ann. § 5322(b); *see Marten v. Godwin*, 499 F.3d 290, 296 (3d Cir. 2007).

Pursuant to the Pennsylvania long-arm statute, this Court may assert personal jurisdiction if the defendants have sufficient "minimum contacts" with this forum and if subjecting the defendants to the court's jurisdiction comports with "traditional notions of fair play and substantial justice." *International Shoe Co. v. Washington*, 326 U.S. 310, 316-17 (1945); *Pinker v. Roche Holdings Ltd.*, 292 F.3d 361, 368-69 (3d Cir. 2002). Where, as here, the cause of action is related to the defendant's contacts with the forum, it is sufficient if the contacts show "purposeful availment" by the defendant of an opportunity to conduct activity in the forum state. *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 475 (1985) ("Jurisdiction is proper . . . where the contacts proximately result from actions by the defendant *himself* that create a "substantial connection" with the forum).

The defendants' victims include individuals and businesses within Pennsylvania. The defendants have not only infected computers in Pennsylvania with Avalanche and the malware systems that traverse it, but have intentionally caused significant harm, and attempted harm in this Commonwealth through bank account intrusions and the stealing of bank funds as well as attempts to do so. In so doing, the defendants have purposefully directed their conduct at Pennsylvania. Accordingly, the defendants' conduct readily satisfies the "minimum contacts" requirement of due process, and personal jurisdiction is consistent with the Pennsylvania long-arm statute, quoted above.

2. The Court Should Authorize Service of Process by Internet Publication

Unless otherwise prohibited by federal law or international agreement, an individual outside the United States may be served "as the court orders." Fed. R. Civ. Pro. 4(f)(3). The method of service selected must be "reasonably calculated, under all circumstances, to apprise interested parties of the pendency of the action" and afford them an opportunity to be heard." *Mullane v. Central Hanover Bank & Trust Co.*, 339 U.S. 306, 314 (1950).

Here, the known administrators of Avalanche, Flux and Flux2, can be served through their jabber account and via publication on the internet. No known physical addresses are available to effect service. The Government will provide notice to Flux and Flux2 through electronic messages. Through the course of the investigation, Jabber addresses used by these defendants have been uncovered by the German authorities and the FBI. The Government will send the Court Filings to these email addresses and Jabber addresses, which should provide these three defendants with notice of this suit.

Further, the Government will post copies of the Court Filings on the websites of the Department of Justice and the FBI (linked to the Department of Justice posting). If the TRO is granted, all press releases issued by the Department of Justice and the FBI with respect to this matter will direct the defendants to the websites where those pleadings can be accessed. Moreover, because the Government's plan to assist victims of Avalanche and the malware systems that traverse it includes substantial media engagement, it is likely that the defendants will learn that the Department of Justice and FBI are involved in the disruption of their infrastructure. There is therefore good cause to believe that the defendants will seek additional information by visiting the public Internet sites of the Department of Justice and FBI and will thereby be notified of this action.

Accordingly, pursuant to Rule 4(f)(3), the Court should approve the Government's plan for service of process.

B. The Court May Authorize the United States to Implement the Technical Disruption Described Above to Stop the Ongoing Fraud and Unlawful Interception of Communications Perpetrated by the Avalanche Botnet

By ordering the relief sought herein, the Court will halt the defendants' use of Avalanche and the malware systems that traverse it to defraud and wiretap U.S. citizens and businesses, and will preserve the status quo while private-sector partners identify and notify victims and assist in removing the defendants' malicious software from their computers.

District Courts generally have broad discretion in deciding whether to grant injunctive relief. *See General Instrument Corp. of Delaware v. Nu-Tek Elecs. & Mfg., Inc.*, 197 F.3d 83, 90 (3d Cir. 1999). As courts of equity, District Courts "'may, and frequently do, go much farther both to give and withhold relief in furtherance of the public interest than they are accustomed to

go when only private interests are involved.' . . . This is especially the case where the public interest in question has been formalized in a statute." *Instant Air Freight Co. v. C.F. Air Freight, Inc.*, 882 F.2d 797, 803 (3d Cir. 1989) (quoting *Virginian Ry. Co. v. System Fed'n No. 40*, 300 U.S. 515, 552 (1937)). In particular, the Third Circuit has noted that injunctive relief is "in the broadest sense for the discretion of the trial court which is best qualified to form a judgment as to the likelihood of a repetition of the offense." *U.S. v. Article of Drug Designated B-Complex Cholinos Capsules*, 362 F.2d 923, 928 (3d Cir. 1966).

Sections 1345 and 2521 of Title 18 enhance the Court's traditional powers at equity by allowing the Court to promptly enjoin ongoing fraudulent or unauthorized interception upon a suit by the Government. These statutes confer broad authorization for courts to enter restraining orders "at any time," or to "take such other action, as is warranted to prevent a continuing and substantial injury." 18 U.S.C. §§ 1354(b), 2521. In particular, Section 1345

> authorizes broad injunctive relief . . . for any violation of chapter 63 [and is] a powerful weapon in the government's anti-fraud arsenal. In addition to authorizing injunctive relief . . . the statute empowers courts to enter restraining orders, prohibitions, and "take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of person for whose protection the action is brought." . . . As a result, civil suits under § 1345 are often used to preserve the status quo during a lengthy parallel criminal probe.

United States v. Payment Processing Ctr., 435 F. Supp.2d 462, 464 (E.D. Pa. 2006); *see also id.* at 466 (citing *United States v. Cen-Card Agency/C.C.A.C.*, No. 88-5764, 1989 WL 30653 (3d Cir. March 23, 1989) (discussing past use of Section 1345 to stop fraud)). Indeed, Congress enacted Section 1345 specifically "to allow the Attorney General to put a speedy end to a fraud scheme by seeking an injunction in federal District Court whenever he determines he has received sufficient evidence of a violation of Chapter 63 to initiate such an action," and intended the

District Court "to grant such action as is warranted to prevent a continuing and substantial injury to the class of persons designed to be protected by the criminal statute." S. Rep. No. 98-225, at 402 (1984). The use of similar statutory language in Section 2521, enacted after Section 1345, suggests a similar Congressional intent to permit the Attorney General to "put a speedy end" to ongoing unlawful interceptions. *See also* S. Rep. No. 99-541, at 34 (1986). The Government seeks the relief set forth herein for precisely those purposes.

Civil injunctive relief, such as that sought in this application, has been used in several Districts to accomplish large-scale disruptions of widespread computer hacking. In some cases, the United States Government has been the plaintiff, and in others, a private party has sought the injunctions. In all cases, injunctions have enabled the plaintiffs to halt hackers' schemes without infringing upon the privacy or property interests of victims or other parties.

For example, in Coreflood, the United States District Court for the District of Connecticut, pursuant to 18 U.S.C. §§ 1345 and 2521, enjoined a series of John Doe defendants from running the Coreflood botnet software.[4] The court based its ruling on the Government's showing that the John Doe defendants were using Coreflood to commit wire and bank fraud and to engage in unauthorized electronic surveillance, that the defendants' conduct was causing a continuing and substantial injury, and that the requested restraining order would prevent or ameliorate that injury. The Coreflood order authorized the FBI to establish a substitute server to

[4] 18 U.S.C. § 1345, combined with the court's inherent equitable authority, was also the basis upon which the U.S. District Court for the Eastern District of Missouri entered a temporary restraining order enjoining individuals from transferring domain names and ordering registrars and registries not to change registration for specified domains, and subsequently entered a permanent injunction with the additional requirement that the registration of defendants' domain names be transferred to non-U.S. registrars. *United States v. Betonsports PLC*. No. 4:06CV01064, 2006 WL 3257797, at *8-9 (E.D. Mo. Nov. 9, 2006); Temporary Restraining Order, *United States v. Betonsports PLC*, No. 4:06CV01064 (E.D. Mo. July 17, 2006).

replace the botnet command and control server formerly run by the defendants and compelled the Domain Registries and Registrars responsible for the domain names used by the Coreflood malware to redirect to the substitute server all traffic intended for the Coreflood domains.

Likewise, in the GameOver Zeus (GOZ) case, *United States v. Bogachev*, No. 2:14-CV-0685 (W.D. Pa., filed May 26, 2014), here in the Western District of Pennsylvania, this District Court enjoined defendants from running the GOZ and Cryptolocker malware again pursuant to 18 U.S.C. §§ 1345 and 2521. The court based its ruling on the Government's showing that the defendants were using GOZ and Cryptolocker to commit wire and bank fraud and to engage in unauthorized electronic surveillance, that the defendants' conduct was causing a continuing and substantial injury, and that the requested restraining order would prevent or ameliorate that injury. The GOZ order, as was the case in Coreflood, authorized the FBI to establish a substitute server to replace the botnet command and control server formerly run by the defendants and compelled the Domain Registries and Registrars responsible for the domain names used by the GOZ and Cryptolocker malware to redirect to the substitute server all traffic intended for the GOZ and Cryptolocker domains.

Similarly, in Microsoft's action against the ZeroAccess botnet, the Western District of Texas entered an injunction granting very similar relief to the relief sought here. Specifically, the Court ordered Domain Registries to redirect traffic from ZeroAccess domains to a substitute command and control server, and ordered 45 U.S. ISPs to block their customers from connecting to a series of malicious IP addresses specified by Microsoft. *See Ex Parte* Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction, *ZeroAccess*, *supra*. Microsoft has obtained similar injunctions in a number of courts throughout the country. *See,*

e.g., *Ex Parte* Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction, *Microsoft Corp. v. Patti et al.*, 1:11 CV 01017 (Sep. 22, 2011); Second Amended *Ex Parte* Temporary Restraining Order, Seizure Order and Order to Show Cause Re Preliminary Injunction, *Microsoft Corp. v. John Does 1-11 Controlling a Computer Botnet Thereby Injuring Microsoft and its Customers*, 2:11 CV 00222 (Mar. 9, 2011); *Ex Parte* Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction, *Microsoft Corp. v. John Does 1-27, Controlling a Computer Botnet Thereby Injuring Microsoft and its Customers*, No. 1:10 CV 156 (E.D.Va. Feb. 22, 2010).

More recently, in the Dridex/Bugat matter, *United States v. Ghinkul, et al.*, No. 2:15-CV-1315 (W.D. Pa., filed October 8, 2015), here in the Western District of Pennsylvania, this District Court enjoined defendants from running a credential harvester that intercepted banking and other online credentials from infected computers and enlisted those computers into a "botnet". The Dridex/Bugat Order authorized the United States to establish computer infrastructure to gain control of the Bugat/Dridex infected computers and directed six companies and organizations to redirect inbound internet traffic from six identified super-peers to Government computers.

1. Statutory Framework

Section 1345 of Title 18 authorizes the Attorney General to commence a civil action for injunctive relief whenever "a person is violating or about to violate this chapter." 18 U.S.C. § 1345(a)(1)(A). The referenced chapter of Title 18 includes Sections 1343 (Fraud by wire, radio, or television) and 1344 (Bank fraud), statutes the defendants are fragrantly violating through the use of Avalanche. Section 1345 further provides that a "permanent or temporary injunction or restraining order shall be granted," and that the "court shall proceed as soon as

practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought." 18 U.S.C. § 1345(a)(3), (b).

Section 2521 of Title 18 similarly authorizes injunctions against illegal interception of communications in violation of 18 U.S.C. § 2511:

> Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of this chapter, the Attorney General may initiate a civil action in a district court of the United States to enjoin such violation. The court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought.

Because Avalanche via the malware systems that traverse it illegally intercept communications between infected computers and Internet websites, Section 2521 also empowers the Government to seek the injunctive relief proposed in this action.

2. The United States May Obtain an Injunction Pursuant to 18 U.S.C. § 1345 and 18 U.S.C. § 2521 Without Demonstrating the Traditional Prerequisites for Injunctive Relief

Where, as here, the United States seeks an injunction pursuant to federal statutes enacted to protect the public interest that provide for injunctive relief, the Court is authorized to issue the injunction if the statutory conditions are satisfied. *See United States v. Nutrition Serv., Inc.*, 227 F. Supp. 375, 388–89 (W.D. Pa. 1964), *aff'd* 347 F.2d 233 (3d Cir. 1965) ("There is sufficient showing [for an injunction], whereas here, the Government presents evidence of violations of the provisions of a statute enacted for the protection of the public. . . . Nor is it necessary to

demonstrate the precise way in which violations of the law might result in injury to the public interest. It is sufficient to show only that the threatened act is within the declared prohibition of Congress."); *United States v. Sene X Eleemosynary Corp.*, 479 F. Supp. 970, 980 (S.D. Fla. 1979) ("Where an injunction is authorized by statute, it is proper to issue such an order to restrain violations of the law if the statutory conditions are satisfied."). The United States thus is not required to demonstrate the traditional prerequisites for a TRO or preliminary injunction, such as irreparable harm or sufficient public interest. *See United States v. Livdahl*, 356 F.Supp.2d 1289, 1290-91 (S.D. Fla. 2005); *Sene X Eleemosynary Corp.*, 479 F. Supp. at 980–81 ("It is sufficient to show only that the threatened act is within the declared prohibition of Congress."); *Nutrition Serv., Inc.*, 227 F. Supp. at 388–89; *see also Government of the Virgin Islands v. Virgin Islands Paving*, 714 F.2d 283, 286 (3d Cir. 1983) (superseded on other grounds by statute, *see Edwards v. Hovensa*, 497 F.3d 355, 359 (3d Cir. 2007); *United States Postal Service v. Beamish*, 466 F.2d 804, 806 (3d Cir. 1972); *CSX Transp., Inc. v. Tennessee Bd. Of Equalization*, 964 F.2d 548, 551 (6th Cir. 1992).[5]

3. The United States Is Authorized to Obtain Injunctive Relief Under 18 U.S.C. § 1345 and 18 U.S.C. § 2521 Because Defendants Are Committing Bank and Wire Fraud and Are Illegally Intercepting Electronic Communications

As detailed in Special Agent Francis' Declaration, and summarized above, the defendants are engaged in wire fraud, bank fraud, and illegal interception of communications on a massive scale through the use of Avalanche and the malware systems that traverse it. The United States is therefore fully authorized to obtain an injunction under both 18 U.S.C. § 1345 and 18 U.S.C. § 2521.

[5] In passing a statute authorizing injunctive relief, Congress implicitly finds that a violation of the law will irreparably harm the public interest. *See Nutrition Serv., Inc.*, 227 F. Supp. at 388–89.

When, as here, a federal statute empowers the Government to obtain an injunction prohibiting further violations of criminal law, courts are split on whether the United States must show that there is probable cause to believe the defendant is violating or is about to violate any of the enumerated offenses, or must demonstrate such violations by a preponderance of the evidence. *Compare United States v. Luis,* 966 F.Supp.2d 1321, 1326 (S.D. Fla. 2013) (probable cause; collecting cases) and *United States v. Payment Processing Ctr., LLC*, 461 F. Supp. 2d 319, 323 & n.4 (E.D. Pa. 2006) (probable cause) with *United States v. Brown*, 988 F.2d 658, 663 (6th Cir. 1993) (preponderance) and *United States v. Williams*, 476 F.Supp.2d 1368, 1374 (M.D.Fla.2007) (preponderance). This issue has not been decided by the Third Circuit. In any event, given the overwhelming evidence of criminal conduct presented in Special Agent Francis' Declaration, the United States easily meets its burden of proof under 18 U.S.C. § 1345 and 18 U.S.C. § 2521 regardless of which evidentiary standard is applied.

a. The Defendants Are Committing Wire Fraud (18 U.S.C. § 1343)

The elements of wire fraud are: (1) a scheme to defraud; (2) use of the wires for the purpose of executing the scheme; and (3) fraudulent intent. *Devon IT, Inc. v. IBM Corp.*, 805 F. Supp. 2d 110, 123 (E.D. Pa. 2011) (citing *United States v. Pharis*, 298 F.3d 228, 234 (3d Cir. 2002)); *see National Sec. Systems, Inc. v. Iola,* 700 F.3d 65, 105 (3d Cir. 2012). Through Avalanche and the malware systems that traverse it, the defendants' conduct readily establishes all of these elements. For example, Corebot captures banking credentials from infected computers through "man-in-the-middle" attacks in which Corebot intercepts sensitive information victims transmit from their computers. 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 through Avalanche.

b. The Defendants are Committing Bank Fraud (18 U.S.C. § 1344)

The elements of bank fraud are: (1) a scheme to defraud a federally insured financial institution; (2) the defendant participated in the scheme by means of false pretenses, representations, or promises that were material; and (3) the defendant acted knowingly. *United States v. Goldblatt*, 813 F.2d 619, 624 (3d Cir. 1987); *McCoy-McMahon v. Godlove*, No. 08-CV-05989, 2011 WL 4820185, at *12 (E.D. Pa. Sept. 30, 2011). The defendants' criminal conduct satisfies each of these elements. Through Avalanche and the malware systems that traverse it, the defendants use botnet to conduct fraudulent financial transfers from federally insured banks, as exemplified by the specific attacks described above. Second, the defendants make materially false representations to both the bank and the victim to perpetrate their fraudulent scheme, both in tricking victims into installing malware and in impersonating victims to conduct the fraudulent transfers. Finally, the defendants act knowingly and intentionally, as demonstrated by their operation of highly sophisticated botnet software to accomplish their fraud.

c. The Defendants are Unlawfully Intercepting Electronic Communications (18 U.S.C. § 2511)

It is a violation of the Wiretap Act to:

> intentionally intercept, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
>
> [or to]
>
> intentionally use, or endeavor to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection.

18 U.S.C. § 2511(1)(a), (d); (4)(a). As described in the Declaration of Special Agent Francis, Avalanche and the malware systems that traverse it are highly advanced communications interception platforms. Through the use of web injects and other tools, these credentials are harvested in real time as they are transmitted from the victim's computer. This conduct clearly violates 18 U.S.C. § 2511(1)(a) and (d).

4. The Proposed Disruption Is Neither A Fourth Amendment Search nor Seizure and Does Not Require the Issuance of a Warrant

The Government's planned disruption of Avalanche and the malware systems that traverse it is neither a search nor a seizure under the Fourth Amendment. Accordingly, this court may authorize the proposed disruption without the issuance of a warrant.

In order to constitute a Fourth Amendment search, the government's actions must either invade an individual's reasonable expectation of privacy, or constitute a physical trespass upon property for the purpose of obtaining information. *See United States v. Jones*, 132 S.Ct. 945, 951 (2012); *Ware v. Donahue*, 950 F.Supp. 2d 738, 744 (D. Del. 2013) (differentiating between a Fourth Amendment search and seizure, and explaining that a "search occurs when an individual's reasonable expectation of privacy is infringed").

Nothing in the planned operation constitutes a Fourth Amendment search. If approved, the only information gathered by the Government during the operation will be dialing,

addressing, routing, and signaling information that will be recorded by the Government when infected computers check in at the substitute servers. There is no reasonable expectation of privacy in this information, which will be collected pursuant to a Pen/Trap Order. *See, e.g. United States v. Christie*, 624 F.3d 558, 573-74 (3d Cir. 2010) ("no reasonable expectation of privacy exists in an IP address"); *United States v. Forrester*, 512 F.3d 500, 510-12 (9th Cir. 2008) (holding that Government surveillance techniques that reveal non-content information, including the to/from addresses of e-mail messages, the IP addresses of websites visited, and the total amount of data transmitted to or from an account, do not constitute a Fourth Amendment search).

The planned disruption also does not constitute a seizure. A seizure occurs when the Government meaningfully interferes with an individual's possessory interests in property. *Soldal v. Cook Cnty.*, 506 U.S. 56, 61 (1992). Here, the proposed operation would cause no meaningful interference with the victims' possessory interests in their computers, or any other possessory interest. If the Court grants the TRO, computers infected with Avalanche and the malware systems that traverse it will be prevented from communicating with computers controlled by the defendants and others involved with the traversing malware systems. The infected computers will begin exchanging routing information with the substitute servers. This transition will be completely transparent to the user, whose computer will perform all authorized functions exactly as it has before. This imperceptible change does not constitute a meaningful interference with the user's possessory interests.

5. *Ex Parte* Relief is Appropriate

The purpose of a temporary restraining order is to preserve the status quo until the Court has an opportunity to pass on the merits of a preliminary injunction. *See Granny Goose Foods,*

Inc. v. Brotherhood of Teamsters & Auto Truck Drivers Local No. 70, 415 U.S. 423, 439 (1974); *Garcia v. Yonkers Sch. Dist.*, 561 F.3d 97, 107 (2d Cir. 2009). A District Court may grant a temporary restraining order without notice to defendants if "specific facts in an affidavit or verified complaint clearly show that immediate and irreparable injury, loss, or damage will result to the movant before the adverse party can be heard in opposition," and the movant "certifies in writing any efforts made to give notice and the reasons why it should not be required." Fed. R. Civ. P. 65(b)(1).

The relief sought herein would preserve the status quo by preventing the defendants from defrauding additional individuals and financial institutions. As discussed herein, the ongoing and aggressive fraud the Government seeks to stop will likely continue to cause irreparable injury and loss until it is halted. Prior notice to the defendants would render futile the Government's efforts to stop the defendants' ongoing criminal acts. If notified in advance of the Government's intended actions, the defendants could and would take simple, rapid steps to blunt or defeat the Government's planned disruption of the Avalanche and the malware systems that traverse it. *See* Francis Decl. ¶__. Such steps would likely include reestablishing their command and control infrastructure and/or making significant changes to the intermediary communication protocols, which would not take extensive time or effort. *Id.* at ¶37. Avalanche and the malware systems that traverse it evolve rapidly, and the Defendants are skilled cyber criminals, easily able to change the structure of Avalanche. *Id.* at ¶__.

The requested *ex parte* relief is necessary to prevent such evasion of the Government's remedial measures. *See* 18 U.S.C. §§ 1345(b) (the "court shall . . . take such other action as is warrant to prevent a continuing and substantial injury"), 2521 (same); Fed. R. Civ. P. 65(b)(1).

6. A Sealing Order Should be Entered in this Case

As set forth in the Government's request for leave to file under seal, the Government respectfully requests leave to file this memorandum, the Complaint, the proposed TRO, and all associated documents under seal. The Government further requests leave to file redacted versions of these documents at the time they are unsealed in order to protect an ongoing law enforcement investigation in this case and similar law enforcement investigations in the future.

Conclusion

For the foregoing reasons, the Government respectfully requests the Court grant the Temporary Restraining Order requested by the Government.

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