Richard A. Jacobsen (RJ5136)
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, New York 10019
Telephone: (212) 506-5000
Facsimile: (212) 506-5151

Gabriel M. Ramsey
(*pro hac vice application pending*)
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, California 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

Attorneys for Plaintiffs
MICROSOFT CORPORATION,
FS-ISAC, INC. and NATIONAL AUTOMATED
CLEARING HOUSE ASSOCIATION

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MICROSOFT CORP., FS-ISAC, INC., and NATIONAL AUTOMATED CLEARING HOUSE ASSOCIATION,

Plaintiffs

v.

JOHN DOES 1-39 D/B/A Slavik, Monstr, IOO, Nu11, nvidiag, zebra7753, lexa_Mef, gss, iceIX, Harderman, Gribodemon, Aqua, aquaSecond, it, percent, cp01, hct, xman, Pepsi, miami, miamibc, petr0vich, Mr. ICQ, Tank, tankist, Kusunagi, Noname, Lucky, Bashorg, Indep, Mask, Enx, Benny, Bentley, Denis Lubimov, MaDaGaSka, Vkontake, rfcid, parik, reronic, Daniel, bx1, Daniel Hamza, Danielbx1, jah, Jonni, jtk, Veggi Roma, D frank, duo, Admin2010, h4x0rdz, Donsft, mary.J555, susanneon, kainehabe, virus_e_2003, spaishp, sere.bro, muddem, mechan1zm, vlad.dimitrov, jheto2002, sector.exploits AND JabberZeus Crew CONTROLLING COMPUTER BOTNETS THEREBY INJURING PLAINTIFFS, AND THEIR CUSTOMERS AND MEMBERS,

Defendants.

CV 12-1335

Case No.

FILED UNDER SEAL

KORMAN, J.

MANN. M.J.

BRIEF IN SUPPORT OF PLAINTIFFS' APPLICATION OF FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER, SEIZURE ORDER AND ORDER TO SHOW CAUSE FOR PRELIMINARY INJUNCTION

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

STATUTES

TABLE OF AUTHORITIES
(continued)

Page(s)

RULES

Plaintiffs Microsoft Corporation ("Microsoft"), the National Automated Clearing House Association ("NACHA") and Financial Services – Information Sharing and Analysis Center ("FS-ISAC") (collectively "Plaintiffs") seek an emergency *ex parte* temporary restraining order ("TRO"), seizure order, and preliminary injunction to halt the growth of the "Zeus", "Ice-IX," and "SpyEye" botnets ("Zeus Botnets") that cause extreme and continued irreparable harm to Plaintiffs, their customers and members, and the general public.

Botnets are computer networks made up of many, in this case **millions**, of end-user computers infected with malicious software. The malicious software puts the infected computer under the control of criminals that transform the infected computers into tools for illicit activity. The criminals controlling botnets can use them for a wide variety of illegal activity – such as stealing consumers' personal information, financial credentials and money, sending spam email, or anonymously conducting other harmful and unlawful activity. Botnets, simply put, are plagues on the Internet, afflicting end users, corporations, and governments alike.

The **Zeus Botnets** are a family of particularly sophisticated and destructive botnets that share common malicious code and a common technical architecture. They have plagued Plaintiffs, financial institutions, consumers and governments for nearly five years. The Zeus Botnets are propagated through a massive spam email scheme that infringes Plaintiffs' trademarks. The Zeus Botnets are designed specifically to intercept, capture, and steal Internet users' online credentials, particularly financial credentials. Defendants controlling the Zeus Botnets use the stolen credentials to access end-users' online-banking accounts and siphon funds. Defendants created and operate the malicious infrastructure at issue in this case. In its five-year history, versions of the Zeus Botnets are estimated to have infected more than **13 million** end-user computers. Unchecked, the botnets will continue to grow and irreparably harm Plaintiffs, their customers and members, governments, and the general public.

The requested TRO directs the disablement and seizure of the Zeus Botnets' command and control servers. These are specialized computers and software residing at specific Internet domains and Internet Protocol (IP) addresses, which send instructions to infected end-user computers and steal online credentials and funds from the victims. The command and control

software operating from and through these domains and IP addresses (hereinafter the "**Harmful Domains and IP Addresses**") instruct infected end-user computers to perform a variety of harmful and illegal acts, including dissemination of email that infects other end-user computers with malware and adds them to the botnet and theft of end-users' personal information such as banking credentials. Disabling the specific Harmful Domains and IP Addresses will sever communication between the command and control servers and the infected end-user computers. Once the command and control servers cannot communicate with infected end-user computers, those infected end-user computers will no longer operate as part of the botnet.

The continued operation of the Zeus Botnets causes severe injury to Plaintiffs and the general public. The Zeus Botnets cause substantial harm by using Plaintiffs' trademarks and brand names in hundreds of millions of spam emails in order to mislead consumers into unknowingly downloading and installing malicious code. In this way, the Zeus Botnets cause irreparable harm to Plaintiffs' goodwill and reputation. Once installed, Defendants use the Zeus Botnets to steal credentials and funds from the victims' computers. Since 2007, it is conservatively estimated that the Zeus Botnets have stolen at least **$100 million** from victims. Plaintiffs, moreover, must divert substantial resources to address the effects of the Zeus Botnets.

Ex parte relief is essential here as notice to Defendants would provide them an opportunity to destroy, move, conceal, or otherwise make inaccessible the instrumentalities used to direct the Zeus Botnets and the primary evidence of their unlawful activity. Defendants can easily redirect infected end-user computers away from the Harmful Domains and IP Addresses if they learn of the impending action. Giving them that opportunity would render further prosecution of this lawsuit entirely fruitless. Equally important, the Harmful Domains and IP Addresses must be disabled simultaneously to prevent one or more Defendants from directing already-infected end-user computers to communicate with alternate command and control servers, allowing the Zeus Botnets to continue to operate and harm Plaintiffs and the public.

The requested *ex parte* relief is not uncommon when disabling dangerous botnets. In a February 2010 case concerning the "Waledac" botnet, the District Court for the Eastern District of Virginia (Judge Brinkema) adopted an approach where:

1) the Court issued a tailored *ex parte* TRO, including provisions sufficient to effectively disable the harmful botnet infrastructure, preserve all evidence of its operations and stop the irreparable harm being inflicted on Microsoft and the public, including Microsoft's customers;

2) immediately after implementing the TRO, Microsoft undertook a comprehensive effort to provide notice of the preliminary injunction hearing and to effect service of process on the defendants, including Court-authorized alternative service by e-mail, electronic messaging services, mail, facsimile, publication and treaty-based means; and

3) after notice, the Court held a preliminary injunction hearing, and granted the preliminary injunction while the case proceeded, in order to ensure that harm caused by the botnet could not continue during the action.

See Microsoft v. John Does 1-27, Case 1:10-cv-00156 (E.D. Va. 2010, Brinkema, J.) (orders attached to Declaration of Jacob M. Heath ("Heath Decl."), Exs. 12, 13.) In March 2011, the District Court for the Western District of Washington adopted a similar approach regarding the "Rustock" botnet. *See Microsoft v. John Does, 1-11,* Case No. 2:11-cv-00222 (W.D. Wash. 2011) (Robart, J.) (Heath Decl., Ex. 14, 15.) In September 2011, the District Court for the Eastern District of Virginia adopted this approach concerning the "Kelihos" botnet. *Microsoft v. Piatti, et al.,* Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.) (Heath Decl., Exs. 16, 17.)

Those approaches are appropriate here. If the Court grants Plaintiffs' requested relief, upon execution, Plaintiffs will immediately make a robust effort in accordance with the requirements of Due Process to provide notice of the preliminary injunction hearing and to effect service of process on Defendants. Plaintiffs will immediately serve the complaint and all papers in this action on Defendants, using known contact information and contact information maintained by the third-party domain registrars and hosting companies that host Defendants' command and control infrastructure.

I. THE ZEUS BOTNETS PROVIDE A SOPHISTICATED PLATFORM FOR CYBERCRIME

The Zeus Botnets are one of the most notorious and widespread information stealing botnet families in existence. The Zeus Botnets are directed primarily at financial data theft (Debenham Decl. ¶¶ 72-77) and their effectiveness has led to the theft of at least $100 million worldwide since 2007. (Declaration of William B. Nelson ("Nelson Decl.") ¶ 15, Ex. 1.) The

Zeus Botnets (1) steal online-banking or other credentials from owners of infected end-user computers, (2) access victims' financial or other accounts with stolen credentials, and (3) siphon funds from the victims' financial accounts to accounts controlled by defendants. (Debenham Decl. ¶ 72-80; Nelson Decl. ¶¶ 16, 17.) Defendants collaborate in a common operation to create, maintain, distribute, and operate the Zeus Botnets. (*See* Debenham Decl. ¶¶ 21-24.)

A. Defendants Create And Operate The Zeus Botnets Through A Continuous, Coordinated Organization.

1. Defendants Who Created The "Zeus," "Ice-IX," And "SpyEye" Code

The Zeus Botnets comprise a family of inter-related botnets – known on the Internet as the "Zeus", "Ice-IX," and "SpyEye" botnets (collectively the "Zeus Botnets"). The Zeus Botnets are built on the same software code and infrastructure. (Debenham Decl. ¶ 23; Declaration of Jesse Kornblum ("Kornblum Decl."), ¶¶ 7, 20-24.) Defendants–whose precise identities are unknown–have operated in anonymity on the Internet for several years. (Debenham Decl. ¶ 21.)

The "Zeus" botnet code first emerged in 2007 when the cyber-security community recognized that it was used to steal information from various organizations. (Debenham Decl. ¶ 13.) John Doe 1, who created the original "Zeus" botnet code, is generally referred to as "Slavik," "Monstr," "IOO," or "Nu11" on anonymous, online cybercrime forums. (Debenham Decl. ¶¶ 12.) The "Zeus" code evolved over time, becoming more sophisticated and including features to counter analysis or disablement of the botnet. (Debenham Decl. ¶¶ 17, 23, 102.) The "Ice-IX" code is built on the "Zeus" code and contains enhancements to avoid virus-scanning software. (Debenham Decl. ¶ 17.) It emerged in the fall of 2011 and was created by John Doe 2, known as "nvidiag", "zebra7753," "lexa_mef," "gss" and "iceIX." (Debenham Decl. ¶¶ 16-17.) The "SpyEye" code was originally independent software, but in October 2010 its creator, John Doe 3, known as "Harderman" or "Gribodemon," announced in online cybercrime forums that it would be merged with the "Zeus" code. (Debenham Decl. ¶ 18-19.) From that point, "Zeus" code and functionality became part of the SpyEye code. (Debenham Decl. ¶¶ 19-20, 23, Exs. 14-18.)

Defendants have offered the botnet code for sale on the Internet as "builder kits" enabling easy setup, operation, maintenance and propagation. (Debenham Decl. ¶ 7.) Builder kits enable

generation of executable code, configuration files and web server files. (*Id.)* John Does 1-3, the creators of the code, offer levels of support for the code once it is sold. Simpler versions with no support may cost as little as $700, where tailored versions with support may cost up to $15,000. (*Id.)*

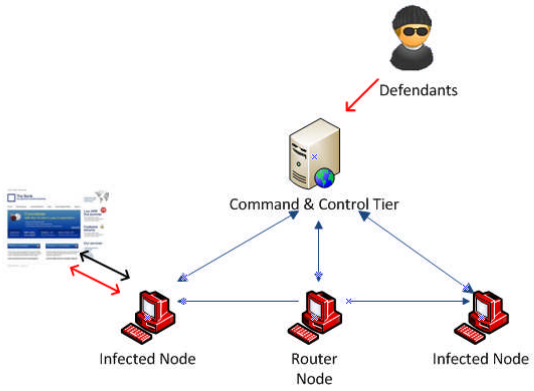
2. Defendant Creators And Purchasers Of The Malicious Code Act In Concert To Operate The Zeus Botnets

John Does 4-39 have purchased or contributed to the Zeus Botnet code and, in concert with the code's creators, are operating the Zeus Botnets. Some Defendants have specialized roles, including: (1) customizing code, (2) creating "web inject" code (a delivery mechanism to introduce botnet code onto victim computers), (3) recruiting "money mules" as intermediaries to create fraudulent bank accounts to which stolen funds are transferred, and (4) acquiring domain names and IP addresses to host the command and control servers. (Debenham Decl., ¶¶ 21, 81.) The common characteristics of botnet code used by these Defendants indicate that they are controlled by the same group of Defendants, who are acting in concert. Plaintiffs' investigation reveals that these Defendants work together in a continuous and coordinated manner to control, operate, distribute, and maintain the Zeus Botnets. (*See* Debenham Decl. ¶¶ 21-24.)

B. The Structure Of The Zeus Botnets

1. The Zeus Botnets Have A Multi-Tiered Architecture

Plaintiffs have carefully studied the Zeus Botnets' architecture, design, and functions. The Zeus Botnets are made up of two tiers of computers: an "Infected Tier," made up of computers infected with Zeus ("Infected Nodes"), some of which have been chosen by the botnet operator to perform additional tasks in managing the botnet ("Router Nodes"), and a "Command and Control Tier." (Debenham Decl. ¶¶ 28-33, 36, 37.) This architecture facilitates the distribution of the botnet malware, propagation of the botnet, and obfuscation of the botnet controllers. (Debenham Decl. ¶¶ 15, 36.) The tiered architecture of the Zeus Botnets can generally be represented as follows:



(Debenham Decl. ¶ 28.)

The lowest tier—the Infected Tier—consists of **millions** of infected end-user computers, of the type commonly found in businesses, living rooms, schools, libraries, and Internet cafes around the world. (Debenham Decl. ¶ 29.) The Infected Tier performs the botnets' daily illicit work. (Debenham Decl. ¶ 33.) Owners of computers in the Infected Tier are targets of Defendants' theft of online credentials, personal information and money from these victims' bank accounts. (*Id.)* Some computers in this tier, the "Router Nodes" are used in some versions of the Zeus Botnets as intermediary computers, relaying communications between different botnet computers and delivering commands and responses among botnet computers. (Debenham Decl. ¶ 36.)

The highest level of the Zeus Botnets architecture—the "Command and Control Tier"—consists of specialized computers and/or software ("servers"). (Debenham Decl. ¶ 37.) Defendants purchase and/or lease these servers to send commands to control the Zeus Botnets' end-user computers of the Infected Tier. (*Id.*)

2. Defendants Use The Harmful Domains And IP Addresses To Infect And Control End-User Computers And To Steal Information And Money From Victims

The servers in the Command and Control Tier are located at the Harmful Domains and IP Addresses identified in Appendices A, B and C to the Complaint. A "domain name" is an

alphanumeric string separated by periods, such as "getbusinessinfo.com," serving as an address for a computer network connection. (Debenham Decl. ¶ 38.) An "IP address" is a unique string of numbers separated by periods, such as "149.154.152.161," that identifies each computer attached to the Internet. (*Id.*) Each active domain name on the Internet has a corresponding IP address where the website content is located. (*Id.*)

Defendants control the Harmful Domains and IP Addresses and use them to distribute and propagate the botnet code, to receive communications from the botnets, and to control the botnets by sending commands to infected computers. (Debenham Decl. ¶¶ 37-39, 116; Kornblum Decl. ¶¶ 7 (c), 25-56.) The *ex parte* relief sought in this motion is directed at disabling these malicious domains and IP addresses. (*See* Debenham Decl., ¶ 109.)

a. Defendants Use The Harmful Domains And IP Addresses To Infect End-User Computers

Defendants use the Harmful Domains and IP Addresses to infect end-user computers, causing them to become part of the Zeus Botnets. (Debenham Decl. ¶ 41; Nelson Decl. ¶ 16; Kornblum Decl. ¶¶ 25-26.) Defendants, for example, may use software called a "Trojan downloader" that installs botnet code onto end-users computers. (Debenham Decl. ¶ 46.) Defendants store this malicious software on servers located at the Harmful Domains and IP Addresses. Defendants mislead Internet users into visiting the Harmful Domains and IP Addresses where users unknowingly download the malicious software. (*Id*., *see also* Moore Decl. ¶¶ 26-32 (explaining evolution of Zeus tactics).) The Harmful Domains and IP Addresses that Defendants use to infect victims' computers are identified in Appendices A through C to the Complaint with the label "Embedded_js," "Infector," "Source," "Dropzone," and "Updater."

Defendants' method of infection involves sending Internet users unsolicited "spam" emails. (Debenham Decl. ¶¶ 47, 85; s*ee also*, Moore Decl. ¶¶ 9-12 (providing details of scope of spam purporting to be from NACHA); *see also*, Johnson Decl. ¶ 8 (defining "spam").) These emails contain links to one or more of the Harmful Domains and IP Addresses. The content of the spam email misleads Internet users to click on the links, causing the malicious software to

be installed on their computers without their knowledge or consent. (Debenham Decl. ¶ 47; Kornblum Decl. ¶¶ 25-26.) Specifically, these spam emails falsely claim to be from Plaintiffs Microsoft and NACHA, the American Bankers Association, financial institutions that are members of Plaintiff FS-ISAC, government agencies, such as the IRS, or other companies. (Debenham Decl. ¶¶ 47-52; Nelson Decl. ¶ 17.) The emails contain Plaintiffs' trademarks and contain misleading messages to induce the user to click on malicious links. (Nelson Decl. ¶ 1; *See e.g.*, Moore Decl. ¶¶ 7, 26, 29, 32.)

For example, Defendants have sent emails purporting to be from Plaintiff Microsoft offering a fake Microsoft "Critical Security Update" and a fake "Update for Microsoft Outlook/Outlook Express," requesting that users click a link. (Debenham Decl. ¶ 48.) Similarly, Defendants send spam emails purporting to be from NACHA requesting that the user click a link to purportedly manage a rejected ACH transaction. (Debenham Decl. ¶ 49; Kornblum Decl. ¶ 25-26; Moore Decl. ¶¶ 7-12.) Other examples include email:

a. purporting to originate from banks and requesting that users click to update their bank information;
b. purporting to be from the American Bankers Association and requesting that the user click on a link to view an account statement;
c. purporting to be from the IRS and requesting that the user click on a link to download a tax statement;
d. purporting to be from DHL or Federal Express and requesting that the user click on a link to confirm a delivery
e. purporting to be an electronic greeting card, inviting users to click on a link to view the card; and
f. purporting to be from social media websites, such as Facebook or others, requesting that users click on a link to accept invitations from "friends."

(Debenham Decl. ¶ 49.) The volume of such spam email is massive. For example, the monthly averages for spam email propagating the Zeus Botnets and infringing NACHA's trademarks *alone* are in the range of one hundred million. (Moore Decl. ¶ 9.) At one point in August 2011, such spam email infringing NACHA's trademarks spiked as high as **167 million emails in a 24 hour period**. (Moore Decl. ¶ 9.) By contrast, the volume of NACHA's normal, authentic outbound email traffic is only 1,500 messages per day. (Moore Decl. ¶ 9; *see also,*

e.g., Johnson Decl. ¶ 20.)

b. Defendants Use The Harmful Domains And IP Addresses To Receive Victims' Stolen Financial Credentials And Other Information

Defendants use many of the Harmful Domains and IP Addresses to collect stolen financial account credentials and other confidential information from infected end-user computers. (Debenham Decl. ¶¶ 53, 79; Nelson Decl. ¶ 17.) The Harmful Domains and IP Addresses that Defendants use to steal such information are identified in Appendices A-C to the complaint with the label "Dropzone." Stolen account credentials are transferred over the Internet from victims' computers to Defendants' computers at the Harmful Domains and IP Addresses. (Debenham Decl. ¶ 53.) Defendants then use this account information to log into victims' accounts and initiate transfers of funds from victims' financial accounts into accounts controlled by the Defendants. (*Id.*; Nelson Decl. ¶ 17.)

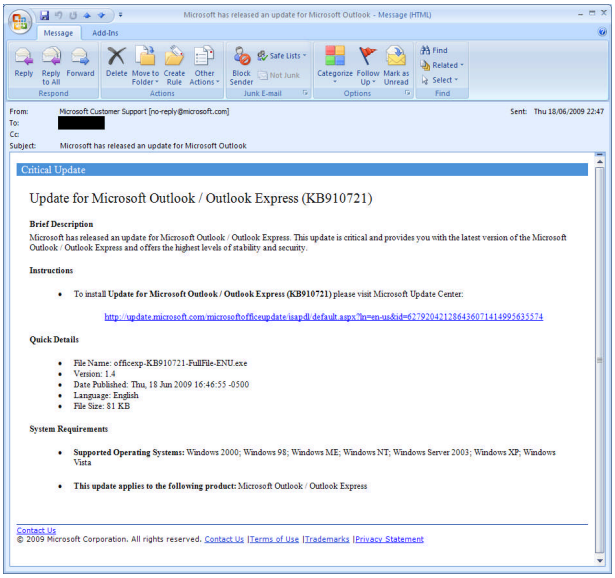
c. Defendants Use The Harmful Domains And IP Addresses To Control The Infected End-User Computers And To Control The Botnet As A Whole

Defendants use the Harmful Domains and IP Addresses to deliver initial or new configurations, instructions and target lists to infected user computers and to control the botnet as a whole. (Debenham Decl. ¶ 54.) In particular, these Harmful Domains and IP Addresses house the Zeus Botnets' "configuration" files. (*Id*. ¶ 55.) The "configuration" files contain templates that mimic the websites of Microsoft, virtually all major financial institutions and other companies. (*Id*. ¶ 56.) Defendants have designed these websites templates to contain not only the trademarks of Microsoft and major financial institutions, but also identical copies of those companies' website content. (*Id*.) Most Internet users are unable to tell the difference between a genuine website and the website templates used by the Zeus Botnets.

The website templates are sent from the Harmful Domains and IP Addresses to infected end-user computers, and when the end-users attempt to access and use their online banking or other websites, the websites templates are presented instead of the genuine website. (Debenham Decl. ¶ 56.) For example, an end-user believes he has accessed his online banking

website and inputs his banking credentials (e.g., name, address, account number, password, social security number, and other identifying information) into the website. (Debenham Decl. ¶¶ 56, 74-78.) In reality, the Zeus Botnets have intercepted the end-user's banking credentials. (*Id.*) The "configuration" files also contain the domain names and IP addresses to which the stolen information is to be sent back. (Debenham Decl. ¶ 56.)

The Harmful Domains and IP Addresses may also contain "spam-templates" or resource files that are sent to infected end-user computers. (Debenham Decl. ¶ 57.) The malicious software on infected end-user computers use these templates to generate spam email that is sent from or through the end-user computers. (*Id.*) The spam is intended to infect other computers and grow the Zeus Botnets. (Debenham Decl. ¶ 47.) The spam templates and resource files stored at the Harmful Domains and IP Addresses contain counterfeit copies of the trademarks of Microsoft, NACHA, American Bankers Association, and FS-ISAC member institutions. (Debenham Decl. ¶ 57.) The following are examples of Defendants' infringement of Microsoft's and NACHA's trademarks (Debenham Decl. ¶ 48):


Microsoft has released an update for Microsoft Outlook - Message (HTML)

Message Add-Ins

Reply Reply to All Forward Delete Move to Folder Create Rule Other Actions Block Sender Safe Lists Not Junk Categorize Follow Up Mark as Unread Find Related Select

From: Microsoft Customer Support [no-reply@microsoft.com]
To: [redacted]
Cc:
Subject: Microsoft has released an update for Microsoft Outlook
Sent: Thu 18/06/2009 22:47

Critical Update

Update for Microsoft Outlook / Outlook Express (KB910721)

Brief Description

Microsoft has released an update for Microsoft Outlook / Outlook Express. This update is critical and provides you with the latest version of the Microsoft Outlook / Outlook Express and offers the highest levels of stability and security.

Instructions

- To install **Update for Microsoft Outlook / Outlook Express (KB910721)** please visit Microsoft Update Center:

http://update.microsoft.com/microsoftofficeupdate/isapdl/default.aspx?ln=en-us&id=627920421286436071414995635574

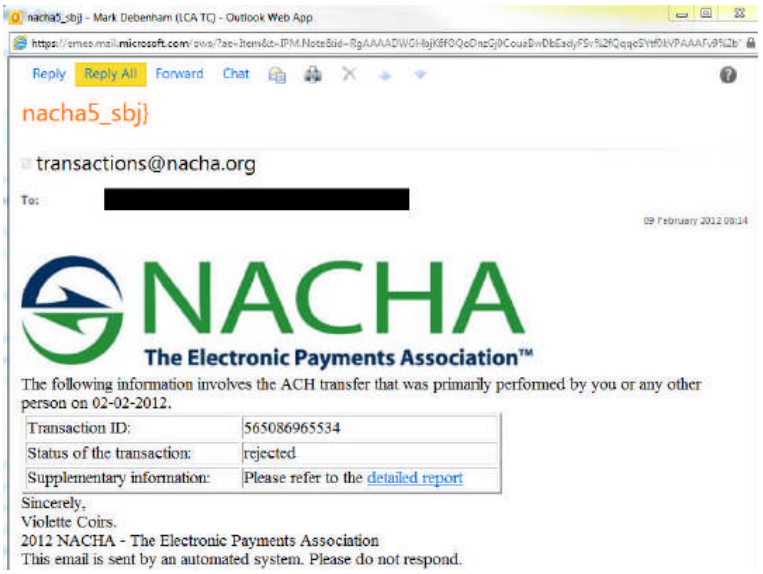
Quick Details

- File Name: officexp-KB910721-FullFile-ENU.exe
- Version: 1.4
- Date Published: Thu, 18 Jun 2009 16:46:55 -0500
- Language: English
- File Size: 81 KB

System Requirements

- **Supported Operating Systems:** Windows 2000; Windows 98; Windows ME; Windows NT; Windows Server 2003; Windows XP; Windows Vista
- **This update applies to the following product:** Microsoft Outlook / Outlook Express

Contact Us
© 2009 Microsoft Corporation. All rights reserved. Contact Us | Terms of Use | Trademarks | Privacy Statement


nacha5_sbj - Mark Debenham (LCA TC) - Outlook Web App

https://emea.mail.microsoft.com/owa/?ae=Item&t=IPM.Note&id=RgAAAADWGHojK6FOQoDnzGj0CouaBwDbEaslyFSv%2FQqqeSYtf0AVPAAAAJv9%2b

Reply Reply All Forward Chat

nacha5_sbj

transactions@nacha.org

To: [redacted]

09 February 2012 06:14

NACHA
The Electronic Payments Association™

The following information involves the ACH transfer that was primarily performed by you or any other person on 02-02-2012.

Transaction ID:	565086965534
Status of the transaction:	rejected
Supplementary information:	Please refer to the detailed report

Sincerely,
Violette Coirs.
2012 NACHA - The Electronic Payments Association
This email is sent by an automated system. Please do not respond.

3. <u>The Zeus Botnets' Command And Control Infrastructure Is Designed To Evade Technical Counter-Measures</u>

The Harmful Domains and IP Addresses represent the most vulnerable point in the Zeus Botnets' architecture. (Debenham Decl. ¶ 59.) Disconnecting the Harmful Domains and IP Addresses and redirecting them to secure computers will sever the botnet's communications

with the infected end-user computers and disable the propagation of the botnet. (*Id.*) Defendants have incorporated features that enable the botnets to better withstand technical counter-measures. (Debenham Decl. ¶¶ 59-61.) For example, over time, the set of domains and IP addresses associated with the command and control servers changes. (Debenham Decl. ¶ 59.) Certain versions of the botnets have fallback mechanisms, use encryption or are designed to evade anti-virus software and common analysis tools. (Debenham Decl. ¶¶ 60-61.) The dynamic nature of the infrastructure makes informal attempts to disable the botnet challenging. (Debenham Decl. ¶59.) Accordingly, as sought in this motion, many such domains and IP addresses must be disabled simultaneously to be effective. (Debenham Decl. ¶¶ 101-108.)

II. THE ZEUS BOTNETS CAUSE SEVERE INJURY TO PLAINTIFFS AND INTERNET USERS

Defendants, the Zeus Botnets and the Harmful Domains and IP Addresses cause severe injury to Plaintiffs and Internet users. Defendants and their malicious infrastructure (1) carry out unauthorized and unlawful intrusion into Microsoft's operating system, Internet users' computers, and the website and email servers of Microsoft and FS-ISAC's financial institution members, (2) infringe the trademarks of Microsoft, NACHA and FS-ISAC's financial institution members, (3) steal Internet users' financial credentials, personal information and money, and (4) use victims' computers to engage in further unlawful conduct.

A. The Zeus Botnets' Malicious Software Installed On Infected Internet User Computers Performs Illicit Acts

Internet users whose computers are infected with the Zeus Botnets' malicious software are damaged by changes that the Zeus Botnets make to the Windows operating system software, altering the normal and approved settings and functions, destabilizing the system, and forcibly drafting customers' computers into the botnet. (Debenham Decl. ¶¶ 62-68.) Once installed on end-users' computers, the malicious botnet software makes changes at the deepest and most sensitive levels of the computer's operating system. (*Id.*) It installs code, intercepts commands and takes unauthorized control of normal Windows processes. (*Id.*) It alters the

behavior of various Windows routines by manipulating registry key settings. (*Id.*) It replaces Windows files with files of the same name that contain the malicious software. (*Id.*)

Once the Zeus Botnets' software infects an end-user computer, it turns the computer into the worker of the botnet, performing the day-to-day illegal activity. The malicious code instructs the computer to, among other things: (a) hide the malware, (b) lower security settings, (c) contact command and control servers to retrieve "configuration files" containing instructions, including website templates that counterfeit the websites and trademarks of Microsoft, FS-ISAC's financial institution members or other companies, (d) in connection with other software, generate spam email that infringe Plaintiffs' and others' trademarks, (e) steal usernames, passwords and other credentials, (f) communicate stolen data back to the command and control servers and (g) intercept or carry out transactions without the user's knowledge or consent. (Debenham Decl. ¶ 70.)

Microsoft's customers are usually unaware that their computers are infected and have become part of the Zeus Botnets. (Debenham Decl. ¶ 69.) Even if they are aware of the infection, they often lack the technical resources or skills to resolve the problem, allowing their computers to be misused indefinitely. (*Id.*) Even with professional assistance, cleaning an infected end-user computer can be exceedingly difficult, time-consuming, and frustrating. (Debenham Decl.; s*ee also* Johnson Decl. ¶ 18 (cost of repairing damage done by identity theft).)

B. <u>The Zeus Botnets Steal Account Credentials And Personal Information</u>

Once installed on an end-user computer, the Zeus Botnet software detects when an Internet user navigates to any website specified in the configuration files, particularly online banking websites. (Debenham Decl. ¶ 74.) Defendants have specified websites ending in "<u>.microsoft.com/,</u>" Microsoft's "<u>hotmail.com</u>" or "<u>live.com</u>" email websites and a variety of online banking sites as targets. (Debenham Decl. ¶¶ 76, 82.) For example, when a user visits their online banking website, the malicious software may do one of the following:

a. Access the real banking website, but unknown to the user, execute instructions that modify or extend the appearance of the website. For example, the software may cause the website to display extra fields into which users are instructed to type sensitive information not actually requested

at the legitimate website. Such manipulated versions of websites may seek information such as "ATM PIN," social security number, mother's maiden name, addresses, birthdates and similar information.

b. Intercept the request from the user's web browser and present a fake, locally generated web page, which appears to be the genuine website, based on the website template retrieved from the command and control server; or

c. Intercept the request and redirect the user to a fake website on the Internet that appears to be the legitimate website.

(Debenham Decl. ¶ 74.) The websites of nearly every major financial institution, Microsoft and a wide array of other Internet companies have been targeted by the Defendants and the Zeus Botnets in this way. (Debenham Decl. ¶¶ 76, 82; Nelson Decl. ¶ 16.) In each case, the website presented to the user is a fake or modified version, which appears very similar to the legitimate website and misuses the trademarks and website content of financial institutions, Microsoft and others. (*See, e.g.*, Debenham Decl. ¶ 75.)

When an Internet user enters his or her account credentials at these websites—*e.g.*, username, password and other additional personal data—Defendants' malicious software intercepts this data and transmits it over the Internet to command and control servers operated at the Harmful Domains and IP Addresses. (Debenham Decl. ¶ 77.) The botnet code is also able to: (1) inject Defendants' own transactions into a victim's online banking session and (2) divert funds from a victim's actual banking or ACH transaction to accounts controlled by Defendants. (Debenham Decl. ¶ 78; Nelson Decl. ¶ 17; *see also* Johnson Decl. ¶ 16 (discussing phishing spam generally).)

Defendants use the victims' account credentials to access their online financial or other accounts and steal money and information. (Debenham Decl. ¶ 79.) Defendants often hire "money mules." These are individuals who travel to different countries, including the United States, in order to set up bank accounts to receive transfers of stolen funds from the victims' accounts. (Debenham Decl. ¶ 81.) They then withdraw funds from the accounts they have set up, keep a percentage for their own payment and transmit the remainder to Defendants. (*Id.*)

The botnet software is specifically designed to allow Defendants to perpetrate this activity without revealing evidence of the fraud until it is too late for the victim to regain control

over funds or stolen information. (Debenham Decl. ¶ 84.) For example, the software can re-write on-screen account balances, generate false account statements, hide transactions from the user's view and can hide itself from antivirus software. (*Id.*)

C. Defendants And The Zeus Botnets Send Spam Email From Or Through End-User Computers

Defendants, through the Zeus Botnets and often in connection with other software, also send unsolicited bulk email (often called "spam" email). (Debenham Decl. ¶ 85.) The spam may be sent from email accounts of victims that Defendants have taken control of using the botnets or sent directly from end-user computers. (Debenham Decl. ¶ 86.) In either situation, such activity is without the knowledge or consent of the victims or the Plaintiffs. (Debenham Decl. ¶¶ 85-87.)

D. Defendants And The Zeus Botnets Severely Injure Microsoft, NACHA and FS-ISAC's Financial Institution Members.

Microsoft provides the Windows operating system, online services such as the "Hotmail" email service, and a variety of other software and websites. (*See* Debenham Decl. ¶¶ 92-93.) It has invested substantial resources developing high-quality products and services. Due to the high quality and effectiveness of Microsoft's products and services and the expenditure of significant resources to market those products and services, Microsoft has generated substantial goodwill with its customers, has established a strong brand, and has developed its name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. Microsoft has registered trademarks representing the source and quality of its products and services and its brand, including "Microsoft," "Outlook" and "Windows" marks.

NACHA is a non-profit association which manages the development, administration, and governance of the ACH Network, the backbone for the electronic movement of money and data. (Moore Decl. ¶ 3.) NACHA represents more than 10,000 financial institutions via 17 regional payments associations and direct membership. (Moore Decl. ¶ 3.) NACHA has developed goodwill with financial institutions, merchants and individual customers and has

established NACHA's name as a strong brand in connection with secure, reliable electronic transactions. (*See* Moore Decl. ¶ 18.) NACHA has registered trademarks representing the source and quality of its services and brand, including "NACHA" and the NACHA logo.

FS-ISAC is a non-profit organization, funded entirely by its members, primarily larger financial services firms, and represents the interests of the financial services sector and financial institution members against cyber and physical threats and risk. (Nelson Decl. ¶¶ 2-6.) FS-ISAC and its financial institution members have made significant investments in developing high-quality, secure online banking and financial services platforms, promoting consumer confidence in those systems and protecting financial institutions and consumers from abuse related to those systems. (*See* Nelson Decl. ¶ 6.) FS-ISAC's members have invested in developing their brands, trademarks and trade names in association with their companies and the financial services they offer. (*See* Nelson Decl. ¶ 16.)

1. Microsoft, NACHA and FS-ISAC Members Are Severely Injured By Spam Email Schemes Carried Out By Defendants And The Zeus Botnets

As a provider of online e-mail services such as Hotmail, Microsoft must maintain spam filters to stop spam from the Zeus Botnets from reaching customers. (Debenham Decl. ¶ 93.) Microsoft's Hotmail systems are the target of a substantial volume of spam from and promoting the Zeus Botnets. (Debenham Decl. ¶ 94.) The spam email to Microsoft's Hotmail email services imposes a burden on Microsoft's servers, and requires Microsoft to expend substantial resources in an attempt to defend against and mitigate the effects of this dangerous email. (*Id.*)

The spam email infringes trademarks of Microsoft, NACHA and FS-ISAC's financial institution members, thus confusing consumers and deceiving them into installing malicious software. (Nelson Decl. ¶¶ 16-17.); *see* Moore Decl. ¶ 18.) Consumers who have been deceived often become angry or frustrated at Microsoft, NACHA or other companies, incorrectly believing them to be responsible for the spam email. (Moore Decl. ¶ 18; Debenham Decl. ¶ 97; *see, e.g.* Johnson Decl. ¶¶ 22-25 (damages to online banking, generally, resulting from fraud).) Plaintiffs must expend resources attempting to remediate consumer confusion

and responding to such confusion. (*See* Debenham ¶¶ 96-98 (discussing at least $1.7 million in cost to Microsoft to investigate and remediate effects of Zeus Botnets).) For example, in merely a one year period, NACHA had to expend $624,000 of its limited resources to combating spam abuse and consumer confusion. (Moore Decl. ¶¶ 18-21 (discussing heavy burden of costs on a relatively small business).)

2. Microsoft, NACHA and FS-ISAC Members Are Severely Injured By Theft Of Account Credentials, Money And Information By Defendants And The Zeus Botnets

The websites of Microsoft and FS-ISAC's financial institution members are directly targeted by Defendants and the Zeus Botnets. (Nelson Decl. ¶ 16.) Defendants steal credentials to access those websites, enabling them to steal personal information from Microsoft users and steal funds from FS-ISAC's financial institution members and their customers. (Nelson Decl. ¶ 16.) Conservatively, since 2007, Defendants and the Zeus Botnets have stolen at least $100 million from victims whose online financial accounts are taken over by Defendants. (Nelson Decl. ¶ 15.)

The Zeus Botnets also make use of counterfeit copies of the trademarks of FS-ISAC's members and Microsoft, including the trade names, logos and website content of those companies, in order to generate fake websites and deceive users into inputting their confidential account information. (Nelson Decl. ¶ 17.) Such activity injures FS-ISAC member institutions and Microsoft, by causing consumer confusion and diminishing their brands and goodwill. (Debenham Decl. ¶ 97; Nelson Decl. ¶ 17.)

Further, Microsoft, as a provider of the Windows operating system and Internet Explorer web browser, must incorporate security features in an attempt to stop account credential theft by the Zeus Botnets from occurring to customers using Microsoft's software. In general, the abuse of Microsoft's, NACHA's and FS-ISAC's members' trademarks to defraud consumers injures the Plaintiffs.

3. Microsoft Is Severely Injured By The High Cost Of Assisting Customers Whose Computers Are Infected By The Zeus Botnets

Microsoft devotes significant computing and human resources to combating infections by

the Zeus Botnets and helping customers determine whether or not their computers are infected, and if so, cleaning them. (Debenham Decl. ¶ 96.) For example, since 2007, Microsoft has detected a staggering 13 million computers infected with some version of the Zeus Botnets. (*Id.*) Microsoft has had to expend substantial resources researching the Zeus Botnets, developing anti-virus filters to combat them, responding to consumer complaints and assisting consumers in cleaning their machines, and investigating and prosecuting enforcement action against the Zeus Botnets. (*Id.*)

III. LEGAL ARGUMENT

Plaintiffs seek an *ex parte* TRO, seizure order and preliminary injunction pursuant to Federal Rule of Civil Procedure 65, Section 1116 of the Lanham Act and the Court's inherent equitable authority to prevent compounding the harm caused by the Zeus Botnets and to maintain the *status quo* by ensuring that evidence of Defendants' misconduct is preserved during the pendency of this case. Plaintiffs' requested relief is warranted here.

A. An *Ex Parte* TRO And Preliminary Injunction Redirecting The Harmful Domains And IP Addresses To Secure Computers Is Warranted

Plaintiffs seek a TRO, seizure order and preliminary injunction pursuant to Rule 65(b) to redirect the Harmful Domains and IP Addresses operating the Zeus Botnets to secure computers, such that they are disabled and the evidence of Defendants' misconduct and damage is preserved. To be eligible for preliminary equitable relief, the movant must establish (1) that it will be irreparably harmed absent temporary injunctive relief and (2) either (a) likelihood of success on the merits or (b) sufficiently serious questions going to the merits to make it fair ground for litigation and balancing of hardships tipping decidedly in its favor. *Winter v. Natural Res. Def. Council, Inc.*, 555 U.S. 7, 24 (2008); *UBS Fin. Servs., Inc. v. W. Va. Univ. Hosps., Inc.*, 660 F.3d 643, 648 (2d Cir. 2011); *Citigroup Global Mkts., Inc. v. VCG Special Opportunities Master Fund Ltd.*, 598 F.3d 30, 35 (2d Cir. 2010). The standard is a flexible one and, in the Second Circuit, preliminary equitable relief is warranted when the movant demonstrates that serious questions going to the merits are raised and the balance of hardships tips sharply in the movant's favor, assuming of course, that the other two *Winter* factors are

met. *UBS Fin. Servs.*, 660 F.3d at 648.

The relief requested by Plaintiffs is warranted. There is a very high likelihood that Plaintiffs will succeed on the merits. Defendants' intrusion into the protected computers of Microsoft, financial institutions and millions of individual victims, theft of hundreds of millions of dollars from innocent Internet users, sending of hundreds of millions of spam emails, and the repeated and deceptive infringement of Plaintiffs' trademarks violates the Computer Fraud & Abuse Act, the CAN-SPAM Act, the Electronic Communications Privacy Act, the Lanham Act, and the Racketeer Influenced and Corrupt Organizations Act. Defendants' deceptive, misleading, and tortious conduct, moreover, violates New York and Washington state law. Plaintiffs and the public will continue to be irreparably harmed if the Zeus Botnets continue to operate through the Harmful Domains and IP Addresses.

At the same time, if the TRO, seizure order and preliminary injunction is issued, no legitimate interests of Defendants will be harmed, and the effect on third-parties (domain registries, IP address hosting companies and free website hosting companies from whom Defendants acquired the Harmful Domains and IP Addresses) will be negligible and short lived. The public interest also weighs heavily in favor of relief because the same injury inflicted on Plaintiffs and their customers by the Zeus Botnets is also visited on the public at large—including government agencies. Accordingly, the relief Plaintiffs request is warranted.

1. Plaintiffs Are Likely To Succeed On The Merits Of Their Claims

Plaintiffs are likely to succeed on the merits of their claims and as such, their request for a TRO and a preliminary injunction should be granted. Plaintiffs' Complaint sets forth the following statutory and common law claims: (1) violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030), (2) violations of the CAN-SPAM Act (15 U.S.C. § 7704), (3) violations of the Electronic Communications Privacy Act (18 U.S.C. § 2701); (4) trademark infringement under the Lanham Act (15 U.S.C. § 1114); (5) false designation of origin under the Lanham Act (15 U.S.C. § 1125(a)); (6) trademark dilution under the Lanham Act (15 U.S.C. 1125(c)), (7) violations of the Racketeer Influenced and Corrupt Organizations Act; (8)

unjust enrichment; (9) trespass to chattels / computer trespass, and (10) conversion.

a. Defendants' The Computer Fraud And Abuse Act Violations

The Computer Fraud and Abuse Act ("CFAA") penalizes, *inter alia*, a party that:

- intentionally accesses a protected computer[1] without authorization, and as a result of such conduct, causes damage (18 U.S.C. § 1030(a)(5)(C)); or
- intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer (18 U.S.C. § 1030(a)(2)(C)); or
- knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer (18 U.S.C. § 1030(a)(5)(A)).

The servers of Plaintiffs and their customers are "protected computers" under the CFAA. Defendants intentionally access Microsoft's proprietary operating system and Microsoft's customers' computers, without authorization, and burden those computers by infecting them with malicious code and executing that code without consent. The Zeus Botnets intentionally access without authorization Plaintiff Microsoft's website servers (to steal users' personal information) and Microsoft's email servers (to send huge volumes of unsolicited, malicious spam email to Microsoft's customers). The Zeus Botnets intentionally access without authorization the website servers of FS-ISAC's financial institution members, in order to access financial accounts and steal funds from these institutions and their customers.

The Zeus Botnets intentional unauthorized access of Plaintiffs' protected computers, moreover, has resulted in substantial damages and loss, including the costs associated with investigating the unauthorized access. The evidence submitted in support of this motion demonstrates that Plaintiffs and their customers and members are damaged by this unauthorized intrusion. Performance of victim computers is degraded by the Zeus Botnets' intrusion. (*See* Debenham Decl. ¶ 89.) Microsoft's email servers are burdened by the sending of an enormous amount of spam email. (Debenham Decl. ¶ 94.) All Plaintiffs must invest considerable time

[1] A "protected computer" is a computer "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communications in the United States." 18 U.S.C. § 1030(e)(2)(B).

and resources investigating and remediating the Defendants' intrusion into these computers. (Debenham Decl. ¶¶ 92, 94.) Microsoft must spend time and resources to combat and remediate infections of user computers caused by the Zeus Botnets. (Debenham Decl. ¶ 96.)

The Zeus Botnets' unauthorized access is precisely the type of activity the Computer Fraud and Abuse Act is designed to prevent. *See e.g. Penrose Computer Marketgroup, Inc. v. Camin*, 682 F. Supp. 2d 202 (N.D.N.Y. 2010); *Global Policy Partners, LLC v. Yessin*, 2009 U.S. Dist. LEXIS 112472, *9-13 (E.D. Va. 2009) (accessing computer using credentials that did not belong to defendant was actionable under the CFAA); *Facebook, Inc. v. Fisher*, 2009 U.S. Dist. LEXIS 122578 (N.D. Cal. 2009) (granting a TRO under CFAA where defendants allegedly engaged in a phishing and spamming scheme that compromised the accounts of Facebook users); *Physicians Interactive v. Lathian Sys., Inc.*, 2003 U.S. Dist. LEXIS 22868, *25 (E.D. Va. 2003) (granting TRO and preliminary injunction under CFAA where the defendant hacked into a computer and stole confidential information).[2] Accordingly, Plaintiffs are likely to succeed on the merits of their Computer Fraud & Abuse Act claims.

b. Defendants' CAN-SPAM Act Violations

The CAN-SPAM Act prohibits, among other acts, the initiation of a transmission of a commercial electronic mail message "that contains, or is accompanied by, header information that is materially false or materially misleading." 15 U.S.C. § 7704(a)(1). Defendants, through the botnet infrastructure, send e-mails containing false "header" information (*i.e.* originating sender, IP address, etc.) making the e-mails appear to originate from addresses purporting to be associated with Microsoft, FS-ISAC's members, and NACHA, or other false addresses, thereby disguising their origin with the purpose of misleading recipients and evading detection. *See* Section II (D) (1)-(2), *supra* pp. 15-16.) This is precisely what CAN-SPAM prohibits. *See Yahoo! Inc. v. XYZ Cos.*, 2011 WL 6072263, * 4 (S.D.N.Y. Dec. 5, 2011) (holding that the transmission of numerous commercial emails with subject headings that misleads recipients

[2] Indeed, in recent years botnet operators who disseminate code that intrudes upon user computers, collects personal information and causes injury have been indicted and convicted criminally under the Computer Fraud & Abuse Act. *See* Heath Decl. ¶ ¶ 38-41, Exs. 10 (Indictment of Jeanson James Ancheta), 11 (Sentencing of Jeanson James Ancheta).

into believing the "Lottery Fraud" emails were authorized by plaintiff and were sent through the plaintiffs servers would violate the CAN-SPAM Act). Plaintiffs are therefore likely to succeed on the merits of its CAN-SPAM Act claim.

c. Defendants' Electronic Communications Privacy Act Violations

The Electronic Communications Privacy Act prohibits "intentionally access[ing] without authorization a facility through which electronic communications are provided" or doing so in excess of authorization and, in doing so, obtaining, altering, or preventing authorized access to an electronic communication while it is in electronic storage. 18 U.S.C. § 2701(a). The servers of Microsoft and FS-ISAC's members are facilities through which electronic communication services are provided. Microsoft's licensed operating systems on end-user computers, moreover, are facilities through which electronic communication services are provided. (*See e.g.*, Debenham Decl. ¶ 90, Fig. 14 (showing connections with other computers attempted by Windows computer).) The Zeus Botnets' malicious code, installed without authorization on infected computers, searches emails and other files, intercepts user communications to and from websites of Microsoft, FS-ISAC's members and other companies, steals the contents of those communications stored on computers, and steals end-user's banking credentials and other information. Once harvested, the stolen credentials are used to steal personal information and money or to send spam email from compromised email accounts. Obtaining stored electronic information in this way, without authorization, is a violation of the Electronic Communications Privacy Act. *See Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC,* 759 F. Supp. 2d 417 (S.D.N.Y. 2010) (holding that an employer's unauthorized access of an employee's personal emails stored on a third-party communication service provider' system violated the ECPA). Plaintiffs, accordingly, are likely to succeed on the merits of their Electronic Communication Privacy Act claim.

d. Defendants' Lanham Act Violations

Section 1114(1) of the Lanham Act prohibits use of a reproduction, counterfeit, copy or "colorable imitation" of a registered mark in connection with the distribution of goods and

services where such use is likely to cause confusion or mistake or to deceive. Defendants distribute copies of Plaintiffs' and their members' registered, famous and distinctive trademarks in fraudulent websites and spam e-mail, which deceive victims, causing them confusion and causing them to mistakenly associate Plaintiffs with this activity. *See* Section (I)(B)(2)(C), *supra* pp. 9-10).

The Zeus Botnet also uses Plaintiffs' and their members registered, famous and distinctive trademarks in website templates and spam templates that Defendants then use to mislead Internet users into providing their website and banking credentials). Defendants steal those credentials and use them to raid Internet users' financial accounts. Defendants' creation and use of counterfeit trademarks in connection with such severe fraud is likely to cause confusion and mistake and to deceive consumers. This is a clear violation of the Lanham Act and Microsoft is likely to succeed on the merits. *Audi AG v. Shokan Coachworks, Inc.*, 592 F. Supp. 2d 246, 279 (N.D.N.Y. 2008) (holding that the use of the plaintiffs' marks in the defendants' email addresses created a likelihood of consumer confusion); *Kuklachev v. Gelfman*, 629 F. Supp. 2d 236, 258 (E.D.N.Y. 2008) (entering preliminary injunction under Lanham Act § 1114 for infringement of trademarks where confusion was likely to result from use of plaintiffs' name and images in connection with defendants' advertisements); *Brookfield Commc'ns. v. W. Coast Entm't Corp.*, 174 F.3d 1036, 1066-1067 (9th Cir. 1999) (entering preliminary injunction under Lanham Act §1114 for infringement of trademark in software and website code).

The Lanham Act also prohibits use of a trademark, any false designation of origin, false designation of fact or misleading representation of fact which:

> is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person.

15 U.S.C. § 1125(a). The Zeus Botnets' misleading and false uses of trademarks—including "Microsoft," "Outlook," "Windows," "NACHA," the NACHA logo, and trademarks of FS-ISAC members such as "Citibank," "Bank of America," "Wells Fargo" and others—causes

confusion and mistake as to Plaintiffs' and their affiliation with the malicious conduct carried out by the botnet. *See* Sections I(B)(2)(C), *supra* pp. 9-10; II (2)(1), pp. 15-16, *supra*. This activity is a clear violation of Lanham Act § 1125(a) and Plaintiffs are likely to succeed on the merits. *See CJ Prods. LLC v. Snuggly Plushez LLC*, 809 F. Supp. 2d 127, 147-48 (E.D.N.Y. 2011) (entering a preliminary injunction under the Lanham Act § 1125(a) for infringement of trademark on a website); *Brookfield Commc'ns.*, 174 F. 3d at 1066-67 (entering preliminary injunction under Lanham Act §1125(a) for infringement of trademark in software and website code); *Hotmail Corp. v. Van$ Money Pie, Inc.*, 47 U.S.P.Q.2d (BNA) 1020,1024, 1025-26 (N.D. Cal. 1998) (granting preliminary injunction; copying the Hotmail trademarks in "e-mail return addresses" constituted false designation of origin); *Am. Online v. IMS*, 24 F. Supp. 2d 548, 551-552 (E.D. Va. 1998) (misuse of trademark in e-mail headers violated §1125(a)).

The Lanham Act further provides that the owner of a famous, distinctive mark "shall be entitled to an injunction against another person" who uses the mark in a way "that is likely to cause dilution by blurring or dilution by tarnishment of the famous mark. . . ." 15 U.S.C. § 1125(c). Here, Defendants' misuse of Plaintiffs' famous marks in connection with malicious conduct aimed at Plaintiffs' customers and the public dilutes the famous marks by tarnishment and by blurring consumers' associations with the marks. This is another clear violation of the Lanham Act, and Plaintiffs are likely to succeed on the merits. *See e.g. Hamzik v. Zale Corp.*, 2007 U.S. Dist. LEXIS 28981 (N.D.N.Y. April 18, 2007); *Hotmail Corp.*, 47 U.S.P.Q.2d at 1024, 1025-26; (spam e-mail with purported "from" addresses including plaintiff's trademarks constituted dilution); *Am. Online*, 24 F. Supp. 2d at 552 (same).

e. <u>Trespass to Chattels/Conversion</u>

A trespass to chattels occurs where a defendant intentionally and without justification or consent, interferes with the use and enjoyment of personal property in the plaintiff's possession and, as a result, causes damages. *Sch. of Visual Arts v Kuprewicz*, 3 Misc. 3d 278, 281 (2003); *Yo! Braces Orthodontics, PLLC v. Theordorou*, 2011 N.Y. Misc. LEXIS 1820, *8 (Apr. 19, 2011). Similarly, conversion occurs where a defendant makes an unauthorized assumption and

exercise of the right of ownership over goods belonging to another, to the exclusion of the owner's rights. *Thyroff v. Nationwide Mut. Ins. Co.*, 8 N.Y.3d 283, 284, 288-89 (2007) (conversion applies to electronic computer records and data).

Defendants have interfered with and taken as their own Plaintiffs' resources, by installing software that interferes with (1) Microsoft's licensed Windows operating system and customer computers and (2) Microsoft's and FS-ISAC's members' website servers, to steal information and money and send vast quantities of spam e-mail. These activities injure the value of Plaintiffs' property and constitute a trespass and conversion. *See Thyroff*, 8 N.Y.3d at 288-89 (conversion of intangible property); *Sch. of Visual. Arts*, 3 Misc. 3d at 282 (sending unsolicited bulk email states claim for trespass to chattels; processing power and disk space adversely affected); *see also Kremen v. Cohen*, 337 F.3d 1024, 1034 (9th Cir. 2003) (hacking into computer system and injuring data supports a conversion claim); *Physicians Interactive v. Lathian Sys.*, 2003 U.S. Dist. LEXIS 22868, at *25, 31 (E.D. Va. 2003) (TRO and preliminary injunction where defendant hacked computers and obtained proprietary information).

f. Unjust Enrichment

The elements of a claim of unjust enrichment are that a (1) defendant benefitted, (2) at plaintiff's expense, and (3) equity and good conscience require restitution. *Beth Israel Med. Ctr. v. Horizon Blue Cross and Blue Shield*, 448 F.3d 573, 586 (2d Cir. 2008). Defendants controlling the Zeus Botnets have benefited from Plaintiffs' trademarks, brand names, and goodwill by, among other things, using Plaintiffs' trademarks, brand names and goodwill to further Defendants' banking fraud on Plaintiffs' customers and members. *See* Section I(B)(2)(a), *supra* pp 7-9.

Defendants have specifically taken, without authorization, the benefit of Microsoft's and FS-ISAC's members' computers in order to steal information and money and send spam email. In each instance, Defendants have profited from their unlawful activity, reaping at least $100 million dollars in stolen money and information. Thus, it is certainly inequitable for Defendants controlling the Zeus Botnets to retain these benefits. Accordingly, Plaintiffs are

likely to succeed on the merits.

g. Defendants' Racketeer Influenced and Corrupt Organizations Act (RICO) Violations

The Racketeer Influenced and Corrupt Organizations Act ("RICO") prohibits "any person employed by or associated with any enterprise engaged in, or the activities of which affect, interstate or foreign commerce to conduct or participate, directly or indirectly, in the conduct of such enterprise's affairs through a pattern of racketeering activity." 18 U.S.C. § 1962(c). RICO also makes it unlawful "for any person to conspire to violate" that provision, regardless of whether that conspiracy ultimately comes to fruition. 18 U.S.C. §1962(d). "Any person injured in his business or property by reason of a violation of" either of these provisions is entitled to recovery, 18 U.S.C. § 1964(c), and this court has "jurisdiction to prevent and restrain" such violations "by issuing appropriate orders." 18 U.S.C. 1964(a). *See also United States v. Carson*, 52 F.3d 1173, 1181-82 (2d Cir. 1995) ("the jurisdictional powers in § 1964(a) serve the goal of foreclosing future violations," and "the equitable relief under RICO is intended to be broad enough to do all that is necessary."); *United States v. Sasso*, 215 F.3d 283, 290 (2d Cir. 2000) (same); *Trane Co. v. O'Connor Sec.*, 718 F.2d 26, 29 (2d Cir. 1983) (preliminary injunction proper under RICO where plaintiff establishes "a likelihood of irreparable harm").

Defendants in this case have formed and associated with such an enterprise affecting foreign and interstate commerce and have engaged in an unlawful pattern of racketeering activity involving thousands of predicate acts of "access device" fraud, 18 U.S.C. § 1029, as well as wire fraud, 18 U.S.C. § 1343 and bank fraud, 18 U.S.C. § 1344.

(1) The Zeus Enterprise

An associated in fact enterprise consists of "a group of persons associated together for a common purpose of engaging in a course of conduct" and "is proved by evidence of an ongoing organization, formal or informal, and by evidence that the various associates function as a continuing unit." *Boyle v. United States*, 556 U.S. 938, 945 (2009). An enterprise requires "at least three structural features: a purpose, relationships among those associated with the enterprise, and longevity sufficient to permit these associates to pursue the enterprise's purpose."

(*Id.*)

The Zeus Enterprise has existed since at least October of 2010, when John Doe 1 and John Doe 3 merged their botnet operations into a single, consolidated global credential stealing botnet. (*See* Debenham Decl. ¶¶ 19, 23.) John Doe 2 joined the conspiracy and began participating in the Zeus Enterprise prior to fall of 2011, when John Doe 2's Zeus variant, "Ice-IX," was released. (*See* Debenham Decl., ¶¶ 16-17, 23.) John Does 4-39 joined and began participating in the Zeus Enterprise at various times thereafter. (Debenham Decl. ¶¶ 22-24.) *See also United States v. Eppolito*, 543 F.3d 25, 49 (2d Cir. 2008) (an enterprise "may continue to exist even though it undergoes changes in membership."). The Zeus Enterprise has continuously and effectively carried out its purpose of developing and operating global credential stealing botnets ever since, and will continue to do so absent the relief Plaintiffs request. (*See* Debenham Decl. ¶¶ 23-24, 26.)

The consolidation of the botnet code and Defendants' interrelated roles in the operation of the Zeus Botnets, in furtherance of common financial interests, demonstrate the purpose of the Zeus Enterprise and the relationship between the Defendants. *Boyle*, 556 U.S. at 945 (relationship and common interest may be inferred from "evidence used to prove the pattern of racketeering activity"); *Eppolito*, 543 U.S. at 50 ("evidence of prior uncharged crimes. . . may be relevant. . . to prove the existence, organization and nature of the RICO enterprise, and a pattern of racketeering activity by each defendant."). The relationship between Defendants may also be inferred by the Defendants' development and/or purchasing of the Zeus botnet code and their use of the Zeus botnet system to steal and exploit customer credentials. (*See* Debenham Decl. ¶ 23.)

(2) <u>Defendants' Pattern of Racketeering Activity</u>

A pattern of racketeering activity "requires at least two acts of racketeering activity, one of which occurred after [October 15, 1970,] and the last of which occurred within ten years. . . after the commission of a prior act of racketeering activity." *H.J. Inc. v. Northwestern Bell Tel. Co.*, 492 U.S. 229, 237 (1989). A threat of continuing activity "is generally presumed when the enterprise's business is primarily or inherently unlawful." *Spool v. World Child Int'l Adoption*

Agency, 520 F.3d 178, 185 (2d Cir. 2008). Defendants have conspired to, and have, conducted and participated in the operations of the Zeus Enterprise through a continuous pattern of racketeering activity. Each predicate act is related and in furtherance of the common unlawful purpose shared by the members of the Zeus Enterprise. These acts are continuing and will continue unless and until this Court grants Plaintiffs' request for a temporary restraining order.

Defendants acts of racketeering activity include access device fraud, in violation of 18 U.S.C. § 1029. Whoever "knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that that period," is guilty of violating 18 U.S.C. § 1029 "if the offense affects interstate or foreign commerce." 18 U.S.C. §1029(a)(2). An "access device" includes "any. . . code, account number, electronic serial number, mobile identification number [or] personal identification number. . . that can be used, alone or in conjunction with another access device, to obtain money. . . or any other thing of value, or that can be used to initiate a transfer of funds." 18 U.S.C. §1029(e)(1). An "unauthorized access device" includes "any access device that is lost, stolen. . . or obtained with intent to defraud." 18 U.S.C. §1029(e)(3). Violation of this statute constitutes "racketeering activity." 18 U.S.C. §1961(1)(B).

Defendants have conspired to, and have, knowingly and with intent to defraud trafficked in thousands of unauthorized access devices in the form of stolen passwords, bank account numbers and other account login credentials through the Zeus botnet system created and operated by Defendants. (*See* Debenham Decl. ¶¶ 12-24.) As set forth in detail above, Defendants have used the Zeus botnet system to intrude upon the computers of Plaintiffs, their members and customers, and steal, intercept and obtain this access device information from thousands of individuals using falsified web pages, and have then used these fraudulently obtained unauthorized access devices to steal *millions* of dollars from these individuals' accounts, in violation of 18 U.S.C. § 1029(a)(2).[3] Each of these illegal acts were conducted

[3] Defendants' conduct also constitutes access device fraud under 18 U.S.C. §1029(a)(3) (possession of unauthorized access devices) and 18 U.S.C. §1029(a)(7) (effecting transactions with unauthorized access devices).

using interstate and/or foreign wires, and therefore affected interstate and/or foreign commerce.[4]

(3) Microsoft's and NACHA's Injury as a Direct Result of Defendants' Pattern of Racketeering Activity

Defendants Botnets have carried out such massive theft by infecting millions of computers running Microsoft's Windows operating system with its malicious software and flooded millions of email accounts, including hundreds of thousands of Microsoft Hotmail email accounts, with spam messages infringing Microsoft's and NACHA's trademarks, and containing links designed to infect computers with malicious software and steal credentials. As a direct result of Defendants' conduct, Microsoft has been forced to spend at least $ 1.7 million to clean infected systems running Microsoft software, mitigate the impact to its customers, and investigate the source of the Zeus botnet and the online identities of Defendants and other members of the Zeus Enterprise. (Debenham Decl. ¶ 98.) As a direct result of Defendants' conduct, NACHA has been forced to spend $624,000 to investigate and combat the activities of the Defendants and the Zeus Enterprise. Accordingly, "there [is] a direct relationship between [the] injury and the defendant's injurious conduct" and "the RICO violation was the but-for (or transactional) cause of [the] injury." *UFCW Local 1776 v. Eli Lilly & Co.*, 620 F.3d 121, 132 (2d Cir. 2010) (citing *Holmes v. Sec. Investor Prot. Corp.*, 503 U.S. 258, 268 (1992)).[5]

2. Irreparable Harm Will Result Unless a TRO and Preliminary Injunction Are Granted

Continued operation of the Zeus Botnets irreparably harms Plaintiffs, their customers and members, and the general public. No monetary remedy could repair the harm to Plaintiffs and Plaintiffs' customers and members if the Zeus Botnets were permitted to continue

[4] Defendants' conduct is also "racketeering activity" in the form of bank fraud under 18 U.S.C. § 1344 (violation where one "knowingly executes, or attempts to execute, a scheme or artifice (1) to defraud a financial institution; or (2) to obtain any of the moneys, funds, credits, assets, securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations, or promises"), and wire fraud under 18 U.S.C. § 1343 (violation where one "having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire. . . communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice.").

[5] Where the pattern of racketeering activity consists of fraud, as here, a plaintiff need not show that it relied on or was deceived by the defendant's fraud – third party reliance is sufficient. *Id.*, *quoting Bridge v. Phoenix Bond & Indem. Co.*, 533 U.S. 639, 657-58 (2008).

operating and expanding. Federal courts addressing botnets have concluded that the "immediate and irreparable harm" to consumers from "botnet command and control servers, spyware, viruses, Trojans, and phishing-related sites; and configuring, deploying and operating botnets," warranted an *ex parte* TRO and preliminary injunction. (*See* Heath Decl., Exs. 16-17 (*Microsoft Corp. v. Piatti, et al.*, Case No. 1:11-cv-1017 (E.D. Va., Cacheris, J.)); Exs. 14-15 (*Microsoft Corp. v. John Does 1-11*, Case No. 2:11-cv-00222 (W.D. Wash. 2011, Robart, J.)); Exs. 12-13, (*Microsoft Corp. v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va., Brinkema J.)); Exs. 8-9 (*FTC v. Pricewert LLC et al.*, Case No. 09-2407 (N.D. Cal., Whyte J.)). These courts have acknowledged the substantial irreparable harm botnets cause Microsoft, its customers and Internet users generally. (Heath Decl., Exs. 8-9, 12-17.)

Plaintiffs, their members and customers, and the public face the same irreparable harm caused by the Zeus Botnets. Thus, entry of an *ex parte* TRO redirecting the Harmful Domains and IP Addresses to secure computers, thus disabling them and preserving evidence of Defendants' misconduct and injury to victims, and an Order to Show Cause why a preliminary injunction should not issue, is warranted. Plaintiffs are irreparably injured because of the problems described above. Customers of Plaintiffs Microsoft and the FS-ISAC members may migrate to other platforms, products or services in the mistaken belief that these institutions are the cause of the problems. Customers may cease conducting online transactions. Once such a switch occurs, given the costs of switching platforms and the uncertainty caused by the botnet in the first place, there is a very high risk that those customers will not return to Microsoft or to the impacted providers of online banking services.

Further, given Defendants' very visible fraud involving infringement of Microsoft's, NACHA's and FS-ISAC's members' trademarks, the Plaintiffs and their members are irreparably injured because the problems created by the Zeus Botnets are improperly attributed to Microsoft, NACHA and FS-ISAC's members. *See* Section II(D)(1), *supra* p. 15). The Defendants' unauthorized use of trademarks in spam emails or on fake web pages in order to deceive consumers and to carry out identity theft and bank fraud diminishes the brands and

goodwill of Microsoft, NACHA and FS-ISAC's members. This causes confusion to consumers, leaving them to attribute the harm to Plaintiffs.

As the Zeus Botnets continue to grow, this harm is compounded. This type of brand related injury and customer harm is most certainly irreparable and is precisely why the relief requested in this motion should be granted. *See Tom Doherty Assocs., Inc. v. Saban Entm't, Inc.*, 60 F.3d 27, 37-38 (2d Cir. 1995) (recognizing that the loss of prospective business or goodwill supports a finding of irreparable harm); *Rex Med. L.P. v. Angiotech Pharms. (U.S.)*, 754 F. Supp. 2d 616, 621 (S.D.N.Y. 2010) (same).

Further, if the requested relief were not granted, the computers of Plaintiffs' customers and members would continue to be infected and the Zeus Botnets would grow. This injury is irreparable because customers and the general public, for the most part, lack the technical knowledge, skills, and ability to remedy the infection or curtail the growth of the Zeus Botnets. In the absence of the requested relief, Plaintiffs' customers and members and the general public would remain under constant threat of their computers being made part of the botnet with the accompanying harmful effects of unauthorized intrusion into and abuse of their computers.

3. The Balance Of Hardships Tips Sharply In Plaintiffs' Favor

Defendants will suffer *no harm* to any legitimate interest if an *ex parte* TRO and preliminary injunction are issued, because it will do no more than preserve the status quo. Redirecting the Harmful Domains and IP Addresses to secure computers will prevent the Zeus Botnets from spreading to any additional computers during that time, and will preserve the evidence of the botnet's structure and illegal activities and evidence of the injury to victims. Plaintiffs have identified no legitimate activities carried on from and through these domains and IP addresses. They serve solely to support the Zeus Botnets. Similarly, there will be only negligible impact on the third-party domain registries, hosting companies and website providers whose services Defendants are using, as the requested relief is carefully tailored to only redirect or disable domains and IP addresses supporting the botnet and directs these third parties to take simple steps, part of their normal operations, to redirect or disable this infrastructure and assist

in preserving evidence.

Conversely, if a TRO and preliminary injunction do not issue, the Zeus Botnets will continue to inflict irreparable injury on Plaintiffs, their customers and members, and the public. The Zeus Botnets are already responsible for at least $100 million in stolen funds from more than 960 banks since 2007, more than 13 million compromised user computers, and sending hundreds of millions of spam e-mail messages. New users are infected each day, dramatically increasing the Zeus Botnets' capacity to carry out illegal conduct, compounding the injury to Plaintiffs, their customers and members, and the public.

Simply put, maintaining the status quo by disabling the Harmful Domains and IP Addresses through which the Zeus Botnets are controlled will not affect any legitimate rights of Defendants. Plaintiffs seek only narrowly tailored assistance from the third-party domain registries, hosting companies and website providers. However, allowing the Zeus Botnets to grow and continue to harm Plaintiffs, their customers and members, and the public while this action is adjudicated poses grave danger to many legitimate interests.

4. The Public Interest Will Be Served By The Issuance Of A TRO And Preliminary Injunction

A TRO and preliminary injunction protects the public interest and not just Plaintiffs and their customers and members because the Zeus Botnets' bank fraud poses serious financial threats to individual consumers and the financial industry. Financial institutions have reported at least $100 million in losses due to the Zeus Botnets. The Zeus Botnets, moreover, target government agencies and websites all over the world. Every website provider, financial institution, government agency, and consumer with access to the Internet or an e-mail platform and the Internet is at risk of being irreparably injured by the Zeus Botnets.

There is an overwhelming public interest in preserving the status quo and halting the growth of the Zeus Botnets while Plaintiffs proceeds with their claims. Two district courts have concluded on three occasions in the last two years that "immediate and irreparable harm" will result to the welfare of consumers from "botnet command and control servers" and the malicious conduct carried out through botnets. (Heath Decl., Exs. 12-17.) Likewise, a TRO

and preliminary injunction here will preserve and protect this important public interest. No such protection will be afforded if preliminary relief is denied and, in that event, the malicious actors controlling the Zeus Botnets will be able to continue their activities with impunity.

5. Only The Requested *Ex Parte* Relief Can Halt The Irreparable Harm To Plaintiffs And The Public

Absent a TRO granting the relief requested herein, the injury to Plaintiffs, their customers and members, and the public will continue unabated, irreparably harming Plaintiffs' reputation, brand and goodwill. The TRO, moreover, must issue *ex parte* for the relief to be effective at all, and the extraordinary factual circumstances here warrant such relief. Rule 65 of the Federal Rules of Civil Procedure permits an *ex parte* TRO where the moving party sets forth facts that show an immediate and irreparable injury and why notice should not be required. Fed. R. Civ. P. 65(b)(1); *see Granny Goose Foods, Inc. v. Teamsters*, 415 U.S. 423, 438-39 (1974) ("Ex parte temporary restraining orders are no doubt necessary in certain circumstances. . . .").

a. If Notice Is Given, The Botnet Will Be Moved And Concealed, Allowing The Harm To Grow And Render Microsoft's Request For Relief Fruitless

If notice is given prior to issuance of a TRO, the Zeus Botnets' command and control infrastructure operating through the Harmful Domains and IP Addresses will be moved to different servers, at different domains and IP addresses, in different areas, enabling Defendants controlling the Zeus Botnets to continue infecting users' computers with malicious software and carrying out the malicious activities described above. Indeed, there is specific evidence that Defendants have evaded prior enforcement attempts, where they had notice, by moving the command and control infrastructure. (*See* Debenham Decl. ¶¶ 101-108.) If Defendants are allowed to do so here, the investigation of the botnet and the illicit activities carried out through it would have to be started anew. (Debenham Decl. ¶¶ 102-108.) Providing notice of the requested TRO will undoubtedly facilitate efforts of the Defendants to evade enforcement efforts.

It is well-established that *ex parte* relief is appropriate under circumstances such as the

instant case, where notice would render the requested relief "fruitless." *See e.g. In re Vuitton Et Fils S.A.*, 606 F.2d 1, 4 (2d Cir. 1979) (*per curiam*) (holding that notice prior to issuing TRO was not necessary where notice would "serve only to render fruitless further prosecution of the action"; prior experience taught that once one member of the counterfeiting enterprise received notice, contraband would be transferred to another unknown counterfeiter, perpetuating the harm and rendering judicial efforts pointless); *Allscripts Misys, LLC v. Am. Digital Networks, LLC*, 2010 U.S. Dist. LEXIS 4450, *2 (D. Md. 2010) (granting an *ex parte* TRO where "Defendant may dissipate the funds and/or take action to render it difficult to recover funds....")

Where there is specific evidence that botnets operators have attempted to and will attempt to evade enforcement attempts when given notice, by moving the command and control infrastructure, courts have repeatedly granted such *ex parte* relief. *See* Heath Decl., Exs. 12, 14, 16 (*Microsoft Corp.*, Case No. 1:10-cv-156 (LMB/JFA) (E.D. Va., Brinkema J.); *Microsoft Corp. v. John Does, 1-11*, Case No. 2:11cv-00222 (W.D. Wash. 2011) (Robart, J.); *Microsoft Corp. v. Dominique Alexander Piatti, et al.*, Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.).)

Also instructive is *FTC v. Pricewert LLC et al.*, where the court issued an *ex parte* TRO suspending Internet connectivity of a company enabling botnet activity and other illegal computer-related conduct on the basis that "[the] Defendant is likely to relocate the harmful and malicious code it hosts and/or warn its criminal clientele of this action if informed of the [plaintiff's] action." (*See* Heath Decl., Ex. 8 (*FTC v. Pricewert LLC et al.*, Case No. 09-2407 (N.D. Cal., Whyte J.).) Moreover, the court in *Dell, Inc. v. Belgiumdomains, LLC*, 2007 U.S. Dist. LEXIS 98676, *4-5 (S.D. Fla. Nov. 21, 2007) issued an *ex parte* TRO against domain registrants where persons similarly situated had previously concealed such conduct and disregarded court orders by, *inter alia*, using fictitious businesses, personal names, and shell entities to hide their activities. (*Id.* at *4.) In Dell the Court explicitly found that where, as in the instant case, Defendants' scheme is "in electronic form and subject to quick, easy, untraceable destruction by Defendants," ex parte relief is particularly warranted. *Id.* at *5-6.

b. If Notice Is Given, Evidence Regarding The Zeus Botnets Will Be Destroyed, Disturbing The Status Quo

If notice is given in advance, evidence of the botnet will be destroyed. In particular, upon notice, the movement of the botnet command and control software will destroy both evidence of the botnet's operation and the injury caused by the botnets. Under such circumstances, courts have issued *ex parte* TROs. *See AT&T Broadband v. Tech Commc'ns, Inc.* 381 F.3d 1309, 1319-1320 (11th Cir. 2004) (affirming *ex parte* search and seizure order to seize contraband technical equipment, given evidence that in the past defendants and persons similarly situated had secreted evidence once notice given); *Dell, Inc*, 2007 U.S. Dist. LEXIS 98676 at *4-5; *Little Tor Auto Center v. Exxon Co., U.S.A.*, 822 F. Supp. 141, 143 (S.D.N.Y. 1993) (*ex parte* TRO appropriate where contraband "may be destroyed as soon as notice is given"). For this reason, the requested *ex parte* TRO is warranted.

B. Only An *Ex Parte* Seizure Order Can Halt The Irreparable Harm To Microsoft And The Public

The Zeus Botnets are specifically designed to resist technical mitigation efforts, eliminating viable technical means to curb the injury. (Debenham Decl. ¶¶ 59-61.) The Zeus Botnets, moreover, are designed to destroy evidence and conceal their misconduct. (Debenham Decl. ¶ 101.) Coupled with Defendants' technological sophistication and expertise in evading enforcement, there is an overwhelming risk that if the most active, current command and control software hosted at the Harmful Domains and IP Addresses are not redirected to secure computers, thus disabling them, and the Defendants' computers at the Harmful IP addresses seized, with the assistance of the United States Marshals Service, Defendants will be able to move the Zeus Botnets, continue their trademark infringement and continue their related activities causing irreparable harm. Thus, the redirection of the Harmful Domains and IP Addresses of the most active, current command and control software to secure computers is warranted.

Section 1116(d) of the Lanham Act provides for *ex parte* seizure and impoundment of infringing and counterfeit items, the instrumentalities used to reproduce the infringing and counterfeit articles, and the records documenting the manufacture, sale and receipt of such

materials. *See* 15 U.S.C. § 1116(d); *Microsoft Corp. v. Jun Yan*, 2010 U.S. Dist. LEXIS 14933, 6-7 (D. Conn. 2010).[6] It is well-established that an *ex parte* seizure order is appropriate where notice would allow defendants to continue their infringement or to destroy, move, hide or otherwise make inaccessible evidence of infringement. *See Microsoft Corp. v. Jun Yan*, 2010 U.S. dis. Lexis 14933 at *1; *AT&T Broadband,* 381 F.3d at 1319; *In re Vuitton Et Fils S.A.*, 606 F.2d at 4. It is also well-settled that courts can impound computers, servers and other electronic data that constitute infringing items, instrumentalities used to carry out infringement, or records of infringement. *See e.g., Dell,* 2007 WL 6862341 at *4-5 (issuing an *ex parte* TRO and seizure order under Section 1116(d) that allowed for a forensic analysis of the defendants' computer data for records).

The Lanham Act authorizes an *ex parte* seizure and impoundment order where the court (1) finds no order other than an *ex parte* seizure is adequate to achieve the purpose of Section 1114; (2) the applicant has not publicized the requested seizure; (3) the applicant is likely to succeed in showing the person against whom seizure would be ordered used the counterfeit mark in connection with the sale, offer for sale or distribution of goods or services; (4) the applicant will suffer irreparable harm; (5) the matter to be seized will be located at the place identified in the application; (6) the balance of hardships tip in favor of seizure; and (7) the persons against whom seizure would be ordered or those working in concert with them would destroy, move, hide or otherwise make such matter inaccessible to the court if the applicant provided notice. *See* 15 U.S.C. § 1116(d)(i)-(vii). Each of these criteria is met in this case.

1. Only Redirecting The Harmful Domains And IP Addresses To Secure Computers, And Seizing The Defendants' Servers At The Harmful IP Addresses Can Ensure That Defendants Will Not Continue Their Activities Or Destroy Or Conceal Evidence

An *ex parte* seizure order redirecting the domains and IP addresses of the most active

[6] *See also Lorillard Tobacco Co. v. Can-Star (U.S.A.) Inc.*, 2005 U.S. Dist. Lexis 38414, *3-4 (N.D. Ill. 2005) ("an *ex parte* motion to search defendants' residences and seize information concerning their finances is the only manner in which to preserve evidence of the location and extent of their assets..."); *Polo Fashions, Inc. v. Clothes Encounters,* 1984 U.S. Dist. Lexis 18196, *8-9 (N.D. Ill. 1984) (*ex parte* TRO appropriate where evidence "relating to the source and the amounts of such merchandise might disappear and the distributor or source of supply thereof remain undetected . . . ").

command and control servers to secure computers is critical to ensure that Defendants cannot continue their deceptive use of Plaintiffs' trademarks and to ensure that Defendants will not destroy or conceal evidence, all of which would render the further prosecution of this action fruitless. Here, there is substantial evidence that if (1) the Harmful Domains and IP Addresses are not redirected to secure computers and (2) Defendants' servers at the Harmful IP Addresses are not physically seized in a highly coordinated manner, Defendants will be able to continue their misleading and illegal use of Plaintiffs' trademarks in the website templates and spam e-mails disseminated by the Zeus Botnets.

The efficacy of such seizure orders against cyber criminals – like Defendants here – is best demonstrated by the Rustock botnet (the largest spam botnet at the time). In a previous enforcement attempt against the Rustock botnet, its operators were able to move the command and control infrastructure during a brief period when the Internet Service Provider inadvertently restored the connection to the domains and IP addresses the Rustock botnet used to communicate with the infected end-user computers. (Heath Decl., ¶ 3.) This allowed the Rustock botnet to continue harming Microsoft and the public for years through spam campaigns. By contrast, a subsequent order issued in a civil action by the District Court for the Western District of Washington, directing seizure of that botnet's command and control servers, resulted in cessation of the botnet's harmful activities.

Such an order in this case is warranted to preserve the evidence, thwart Defendants' continued operation of the Zeus Botnets and protect against inadvertent or intentional acts by any third party that would enable Defendants to continue their activities and/or destroy evidence of the operation of Zeus Botnets.

2. Plaintiffs Will Not Publicize The Requested Seizure In Advance

Other than notifying the United States Attorney for the Eastern District Of New York, the United States Marshals Service in districts where seizure is to be effected and preparing for service of process after any order is executed, pursuant to Section 1116(d)(2) of the Lanham Act, Plaintiffs have not and will not publicize the requested seizure until after the requested

seizure is carried out. (Heath Decl. ¶ 17.)

3. Plaintiffs Are Likely To Succeed On The Merits Of Its Trademark Infringement Claim

As discussed the Zeus Botnets' command and control infrastructure hosted at the Harmful Domains and IP Addresses contain website templates and spam templates that make infringing use of counterfeit Plaintiffs trademarks, including but not limited to those attached as Appendices D and E to the Complaint. The command and control infrastructure operating at the Harmful Domains and IP Addresses also makes infringing use of counterfeit Plaintiffs trademarks by sending spam email that contain such counterfeit trademarks and by generating fake websites that contain such counterfeit trademarks in order to deceive Internet users. This constitutes trademark infringement and false designation of origin under Sections 1114 and 1125(a) of the Lanham Act. The command and control infrastructure and software hosted at and operating through the Harmful Domains and IP Addresses both contain counterfeit trademarks and are instrumentalities used to carry out the infringement. Thus, Plaintiffs are likely to succeed on the merits and the command and control software is subject to seizure and impoundment under Section 1116(d) of the Lanham Act.

4. Immediate And Irreparable Injury Will Occur If An *Ex Parte* Seizure Order Does Not Issue

As discussed above Plaintiffs, their members and their customers, and the public will continue to suffer irreparable harm if the Zeus Botnets are allowed to continue growing through the infringement of Plaintiffs' trademarks and are allowed to carry out its malicious activities.

5. The Material To Be Seized And The Locations To Be Searched Are Identified In The Application

In its proposed TRO and seizure order, Plaintiffs identify with specificity the items to be seized and the places where Defendants' command and control infrastructure for the Zeus Botnets can be found. The proposed order identifies the following:

A. Appendix A to the proposed order identifies Defendants' specific harmful domains (domains such as "fastspy.info," "nacha-reports.org," "ijqrqinymhjsvr.net"

and others) and identifies the specific domain registries through which Defendants registered the domains. The domain registries are directed to redirect Defendants' Harmful Domains to specific IP addresses of secure computers, in order to disable those domains and preserve evidence available through them;

B. Appendix B to the proposed order identifies Defendants' specific harmful IP addresses and identifies the specific data centers and hosting companies in two locations through which Defendants registered the IP addresses. The hosting companies are directed to redirect Defendants' Harmful IP Addresses to secure computers, in order to preserve evidence available through them and thereafter disable them prevent the abuse currently carried out through the IP addresses.

C. Appendix C to the proposed order identifies very specific harmful file paths—such as http://qybo-hubybewu.freewebsitehosting.com/nonplatentiluu21.html—that Defendants created through free website hosting services (in this case the service is called "freewebsitehosting.com"). In these cases, the free website hosting services are directed to delete or otherwise disable access to the full file path. The general domain of the website hosting service (freewebsitehosting.com or other examples) may remain in operation as Defendants' malicious activity only takes place at the very specific listed file paths and files.

Regarding the computers and related materials to be seized at the hosting companies, the proposed order directs the U.S. Marshals Service to carry out service of the order and direct redirection of the IP addresses and seizure of the computers, servers, electronic data storage devices, software, data or media that correspond to the Harmful IP Addresses assigned to Defendants. This material is readily ascertainable because each IP address corresponds to computers in the hosting companies' possession, custody or control. The proposed order directs the hosting companies to redirect the IP addresses to secure computers and isolate and turn over to the U.S. Marshals Service the botnet software and related content on the computers associated with these domains and IP addresses.

The proposed order also identifies categories of records and documents to be seized or

provided, including information relating to the identity of Defendants using the Harmful IP Addresses and all logs associated with these servers, all of which is readily ascertainable. This information will enable Plaintiffs to effect notice and service of process on Defendants.

These categories are sufficiently specific to allow the U.S. Marshals Service, the hosting company and third-party forensic experts under contract with Plaintiffs to locate the material to be seized without undue burden. As Plaintiffs anticipate that some of the material to be seized will be electronic data files, it requests the Court to issue a writ of assistance allowing forensic experts to assist with identification of electronic data and media that contain the malicious code. A district court has the power to issue a writ of assistance that compels third parties with technical skills to assist in the technical implementation of a court's order. *See Dell, Inc.*, 2007 WL 6862341 at *4 (citing *United States v. New York Tel. Co.*, 434 U.S. 159, 176 (1977)). The third-party experts will hold the material in secure escrow as the case proceeds.

6. The Harm To Plaintiffs And The Public Of Denying The Requested Relief Outweighs The Harm To Any Legitimate Interests Of Defendants

As previously established, if the requested relief is denied, serious and irreparable harm to Plaintiffs, their customers and members, and the public will result. By contrast, Defendants will suffer no harm to any legitimate interest if an *ex parte* TRO and seizure Order issues, as the malicious Zeus Botnets' command and control code operating from the servers at those Harmful Domains and IP Addresses is used solely to propagate and control the Zeus Botnets and not for any legitimate or lawful purpose. Further, as discussed, the impact of the requested relief to the third party domain registries, hosting companies and website providers will be negligible, as the order disables access to only a handful of their customers engaged in illegal conduct and seeks these companies' reasonable assistance in the isolation and seizure of the botnet code.

Because each unique Harmful Domain or IP Address is associated with a specific command and control server, identifying and isolating the malicious code onto secure

computers and disabling that code should result in only minimal burden to the domain registries, hosting companies and website providers. The actions requested are well within the ordinary course of these companies' activities generally and their abuse response activities specifically. Plaintiffs, moreover, will utilize forensic experts to expedite the seizure and further minimize any potential burden. Finally, there will be no impact of the requested relief on any other parties. The Harmful Domains are all solely used by Defendants to carry out the botnet and investigation has revealed only botnet-related activity related to the Harmful IP Addresses. If any third party were found to host content on any of the IP Addresses listed, the impact would be negligible. Such content can be quickly and readily moved by the relevant hosting provider to another IP address and the owners/operators of the content can be promptly notified of the change in IP address. Microsoft and its counsel have carried out such orders successfully in the past, using the same methods sought here.

7. Defendants Are Likely To Destroy, Move, Hide Or Conceal Evidence If Provided Notice

As discussed in detail, Defendants are likely to remove the malicious code and relocate it to new servers if they are provided notice. As such, an *ex parte* TRO and seizure order redirecting the Domains and IP Addresses to secure computers and directing seizure of Defendants' command and control servers is necessary.

8. The All Writs Act Authorizes The Court To Direct Third Parties To Perform Acts Necessary To Avoid Frustration Of The Requested Relief

Plaintiffs' Proposed Order directs that the third-party domain registries, IP address hosting companies and free website providers, through which Defendants procured the Harmful Domains and IP Addresses, reasonably cooperate to effectuate the order. Critically, these third-parties are the only entities that can effectively disable Defendants' domains and IP addresses and preserve the evidence, and thus their cooperation is necessary.

The All Writs Act provides that a court may issue all writs necessary or appropriate for the administration of justice. 28 U.S.C. § 1651(a). The Supreme Court has recognized that narrow direction to third-parties necessary to effect the implementation of a court order is

authorized by the All Writs Act:

> The power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice, and encompasses even those who have not taken any affirmative action to hinder justice.

United States v. New York Tel. Co., 434 U.S. at 174 (citations omitted) (order to telephone company to assist in implementation of a pen register warrant was authorized under the All Writs Act); *see also In re Application of United States for an Order Authorizing An In-Progress Trace of Wire*, 616 F.2d 1122, 1129 (9th Cir. 1980) (same; noting of *New York Tel.Co.*, "the Court made the commonsense observation that, without the participation of the telephone company, 'there is no conceivable way in which the surveillance authorized could have been successfully accomplished.'"); *In re Baldwin-United Corp.*, 770 F.2d 328, 338-339 (2d Cir. 1985) ("An important feature of the All-Writs Act is its grant of authority to enjoin and bind non-parties to an action when needed to preserve the court's ability to reach or enforce its decision in a case over which it has proper jurisdiction"; "We do not believe that Rule 65 was intended to impose such a limit on the court's authority provided by the All-Writs Act to protect its ability to render a binding judgment."); *Dell Inc. v. BelgiumDomains, LLC*, 2007 U.S. Dist. LEXIS 98676 (S.D. Fla. Nov. 20, 2007) (All Writs Act applied in conjunction with trademark seizure under Rule 65 and Lanham Act).

Requiring these third parties to reasonably assist in the execution of this order will not offend due process as the Proposed Order requires (1) only minimal assistance from the third parties in executing the order (acts that they would take in the ordinary course of their operations), (2) that it be implemented with the least degree of interference with the normal operation of third parties, (3) does not deprive the third parties of any tangible or significant property interests and (4) requires Plaintiffs to compensate the third-parties for the assistance rendered. If, in the implementation of the Proposed Order, any third-party wishes to bring an issue to the attention of the Court, Plaintiffs will bring it immediately. The third-parties, moreover, will have an opportunity to be heard at the preliminary injunction hearing, which

must occur shortly after the execution of the Proposed Order. Fed. R. Civ. P. 65(b)(2). The directions to third-parties in the Proposed Order are thus narrow, satisfy due process, and are necessary to effect the requested relief and ensure that the relief is not rendered fruitless.

C. Plaintiffs Will Make Extraordinary Efforts To Provide Notice Of The TRO And The Preliminary Injunction Hearing And To Serve The Complaint

To ensure Due Process, immediately upon entry of the requested *ex parte* TRO, Plaintiffs will undertake extraordinary efforts to provide formal and informal notice of the preliminary injunction hearing to Defendants and to serve the complaint. In order to carry out service, the proposed TRO also directs the relevant hosting companies and domain registrars/registries to provide all contact information for the Defendants through which notice may be provided.

Courts in the Second Circuit permit discovery to determine the identity of unknown defendants. *Digital Sin, Inc. v. Does 1-176,* 2012 WL 263491 *2 (S.D.N.Y., Jan. 30, 2012) (allowing discovery of unknown defendants where plaintiff made *prima facie* case of copyright infringement and no other means of obtaining the identity of the alleged infringers). The Second Circuit employs two tests for determining whether to provide expedited discovery. The first is a "reasonableness standard" (*see Keybank, Nat'l Assoc. v. Quality Pay-Roll Sys., Inc.* 2006 WL 1720461, at *4 (E.D.N.Y. Jun. 22, 2006)) and a four-factor test that requires a showing of (1) irreparable injury; (2) some probability of success on the merits; (3) some connection between the expedited discovery and the avoidance of irreparable harm; and (4) some evidence that the need for the expedited discovery outweighs the injury defendants will suffer from the expedited discovery. *Notaro v. Koch,* 95 F.R.D. 403 (S.D.N.Y. 1982).

The discovery requested here is reasonable as it is necessary to identify Defendants in order to serve them and hold them accountable for their unlawful conduct. Defendants are real people who have created and now direct the daily operation of the Zeus Botnets. If identified, they will be amenable to suit in federal court. Plaintiffs have diligently researched the Zeus Botnets, and have identified the Harmful Domains and IP Addresses that comprise the Command and Control Tier of the botnet set up by Defendants. Plaintiffs' investigation into

Defendants' identities can progress no further until it gains access to more information related to the specific identities of the Defendants. The requested information is necessary to identify the Defendants, serve them with process, and prosecute this case.

Plaintiffs also satisfy the four-factor test. As established, Plaintiffs will be irreparably harmed as long as the Zeus Botnets continue to operate and have demonstrated a probability of success. The requested discovery bears directly on the irreparable harm. While disabling the Harmful IP Addresses and Domains will cease the immediate risks of the botnets, Defendants still have possession of information already stolen and may continue to use that information to perpetrate further harm. The injury resulting from denying the requested discovery would outweigh any impact of Defendants' interests from granting the relief. At this point in the proceedings, Plaintiffs' requests for contact information will be made only to service providers providing support for the critical botnet infrastructure. Accordingly, good and compelling cause exists to grant Plaintiffs' narrow request for Doe discovery.

Plaintiffs Will Provide Notice By E-mail, Facsimile, Mail: Plaintiffs will provide notice of the preliminary injunction hearing and will effect service of the Complaint by immediately sending all pleadings to the e-mail and messaging addresses, facsimile numbers and mailing addresses associated with Defendants or provided by Defendants to domain registrars/registries and hosting companies in relation to the command and control infrastructure. When Defendants registered for domain names and hosting services, they agreed not to engage in abuse such as that at issue in this case and agreed that notice of disputes regarding domain or IP address hosting could be provided to them by sending complaints to the e-mail, facsimile and mail addresses provide by them. (*See* Heath Decl. ¶¶ 11, 22-35.)

Plaintiffs Will Provide Notice To Defendants By Publication: Plaintiffs will notify the Defendants of the preliminary injunction hearing and the complaint against their misconduct by publishing the materials on a centrally located, publically accessible source on the Internet for a period of 6 months. Plaintiffs will effect notice by publication in general circulation newspapers in Russia, Ukraine & Romania where Defendants' are generally

believed to reside. Plaintiffs will also affect notice by additional methods as may be directed by the Court.

Plaintiffs Will Provide Notice By Personal Delivery And Treaty If Possible: If valid physical addresses of Defendants can be identified, Plaintiffs will notify Defendants and serve process upon them by personal delivery or through the Hague Convention on service of process or similar treaty-based means.

Notice and service by the foregoing means satisfy Due Process, are appropriate, sufficient and reasonable to apprise Defendants of this action and are necessary under the circumstances. Plaintiffs hereby formally request that the Court approve and order the alternative means of service discussed above. The Court can order Plaintiffs' proposed methods of notice and service under Federal Rule of Civil Procedure 4(f)(3) which authorizes service by "other means" that are "not prohibited by international agreement." *Gurung v. Malhotra,* --- F.R.D. ---, 2011 WL 5920766, * 2 (S.D.N.Y. Nov. 22, 2011). A party need not have attempted every permissible means of service before petitioning the court for alternative relief under Rule 4(f)(3) as it stands on equal footing with other methods of service Rule 4 authorizes. *See Ryan v. Brunswick Corp.,* 2002 WL 1628933, *2 (W.D.N.Y. May 31, 2002) (Rule 4(f)(3) "is neither 'extraordinary relief' nor a 'last resort' to be used only when parties are unable to effectuate service under (f)(1) or (f)(2)").

In this case, the e-mail addresses provided by Defendants to the domain registrars / registries and hosting companies, in the course of obtaining services that support the botnet, are likely to be the most accurate and viable contact information and means of notice and service. (Heath Decl. ¶ 10.) Defendants, moreover, will expect notice regarding their use of these services to operate their botnet by those means, as Defendants agreed to such in their domain registration and hosting agreements. *See Nat'l Equip. Rental, Ltd. v. Szukhent,* 375 U.S. 311 (1964) ("And it is settled. . . that parties to a contract may agree in advance to submit to the jurisdiction of a given court, to permit notice to be served by the opposing party, or even to waive notice altogether."); *Ryan,* 2002 WL 1628933 at *2 (authorizing service by regular mail

where defendant's website directed parties to communicate with it through regular mail). For these reasons, notice and service by e-mail and publication are warranted and necessary here.[7]

Plaintiffs' proposed methods of notice and service by e-mail, facsimile, mail and publication also satisfy Due Process as these means are reasonably calculated, in light of the circumstances, to apprise the interested parties of the TRO, the preliminary injunction hearing and the lawsuit. *See Mullane v. Cent. Hanover Bank & Trust Co.*, 339 U.S. 306, 314 (1950). *See e.g., Ryan*, 2002 WL 1628933 at *2 (authorizing service by regular mail, fax and/or email); *Smith v. Islamic Emirate of Afghanistan*, 2001 U.S. Dist. LEXIS at * 8-11 (authorizing service by publication upon Osama bin Laden and the al-Qaeda organization); *Rio Prop., Inc.*, 284 F.3d at 1014-15 (authorizing service by e-mail upon an international defendant); *FMAC Loan Receivables v. Dagra*, 228 F.R.D. 531, 535-36 (E.D. Va. 2005) (acknowledging that courts have readily used Rule 4(f)(3) to authorize international service through non-traditional means); *BP Prods. N. Am., Inc. v. Dagra*, 236 F.R.D. 270, 271-73 (E.D. Va. 2006) (approving notice by publication); *AllscriptsMisys, LLC*, 2010 U.S. Dist. LEXIS 4450, at *3 (granting *ex parte* TRO and order prompting "notice of this Order and Temporary Restraining Order as can be effected by telephone, electronic means, mail or delivery services."); *Microsoft Corp. v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va. 2010, Brinkema J.) at Dkt. 38, pg 4 (authorizing notice of preliminary injunction and service on botnet operators by e-mail, facsimile, mail and publication).

Such service is particularly warranted in cases such as this involving Internet-based misconduct, carried out by international defendants, causing immediate, irreparable harm. As the Ninth Circuit recently observed:

> [Defendant] had neither an office nor a door; it had only a computer terminal. If any method of communication is reasonably calculated to provide [Defendant] with notice, surely it is e-mail-the method of communication which [Defendant] utilizes and prefers. In addition, e-mail was the only court-ordered method of

[7] Additionally, if the physical addressees provided by Defendants to hosting companies turns out to be false and Defendants' whereabouts are unknown, the Hague Convention will not apply in any event and alternative means of service, such as email and publication, would be appropriate for that reason as well. *See BP Prods. N. Am., Inc.*, 236 F.R.D. at 271 ("The Hague Convention does not apply in cases where the address of the foreign party to be served is unknown.")

> service aimed directly and instantly at [Defendant]. . . Indeed, when faced with an international e-business scofflaw, playing hide-and-seek with the federal court, e-mail may be the only means of effecting service of process.

Rio Props., Inc., 284 F.3d at 1014-1015; *see also Williams-Sonoma, Inc. v. Friendfinder, Inc.*, 2007 U.S. Dist. LEXIS 31299, *5-6 (N.D. Cal. 2007) (service by e-mail consistent with Hague Convention and warranted in case involving misuse of Internet technology by international defendants).

For all of the foregoing reasons, Plaintiffs respectfully request that the Court enter the requested TRO, seizure order and order to show cause why a preliminary injunction should not issue, and further order that the means of notice of the preliminary injunction hearing and service of the complaint set forth herein meet Fed. R. Civ. Pro. 4(f)(3), satisfy Due Process and are reasonably calculated to notify Defendants of this action.

IV. CONCLUSION

For the reasons set forth herein, Plaintiffs respectfully request that this Honorable Court grant their motion for a TRO, seizure order and order to show cause regarding a preliminary injunction. Plaintiffs further respectfully request that the Court permit notice of the preliminary injunction hearing and service of the Complaint by alternative means.

Dated: March 18, 2012

Respectfully Submitted,

ORRICK, HERRINGTON & SUTCLIFFE LLP

By: _____

Richard A. Jacobsen
51 West 52nd Street
New York, NY 10019
Tel: (212) 506-5000
Fax: (212) 506-5151
Attorneys for Plaintiffs
Microsoft Corporation
FS-ISAC, Inc.
National Automated Clearing House Association