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
(admitted *pro hac vice*)
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, D frank, duo, Admin2010, h4x0rdz, Donsft, mary.J555, susanneon, kainehabe, virus_e_2003, spanishp, sere.bro, muddem, mechan1zm, vlad.dimitrov, jheto2002, sector.exploits AND JabberZeus Crew, AND YEVHEN KULIBABA AND YURIY KONOVALENKO, CONTROLLING COMPUTER BOTNETS THEREBY INJURING PLAINTIFFS, AND THEIR CUSTOMERS AND MEMBERS,

Defendants.

Hon. Sterling Johnson, Jr.

Case No. 12-cv-01335 (SJ/RLM)

MOTION FOR ENTRY OF DEFAULT PURSUANT TO FEDERAL RULE OF CIVIL PROCEDURE 55(a) AND LOCAL CIVIL RULE 55.1

Plaintiffs Microsoft Corporation, FS-ISAC, Inc., and the National Automated Clearing House Association (collectively, "Plaintiffs"), respectfully request, pursuant to Fed. R. Civ. P. 55(a) and Local Civil Rule 55.1, that the Court enter default against John Doe Defendants 1-21, 25-35, 37-39 ("Defendants") who operated and controlled the Zeus botnets from and through the Internet domains at issue in this case.[1] Entry of default is warranted here. Plaintiffs served Defendants with the Complaint, Amended Complaint, summons and related materials through Court-ordered methods pursuant to Fed. R. Civ. P. 4(f)(3) that were reasonably calculated to provide Defendants with notice of these proceedings. Defendants received notice and are very likely aware of these proceedings, and despite receiving notice have not appeared in this action.

In the Temporary Restraining Order and preliminary injunction, the Court authorized service of the Complaint and summons by alternative means pursuant to Rule 4(f)(3). The Court approved alternative means of service, including service by publication and by electronic means, which would satisfy the requirements of Due Process and are reasonably calculated to notify Defendants of this action and provide them the opportunity to respond. Plaintiffs used these methods of service to notify Defendants of this action. None of the Defendants have, however, answered or otherwise responded in the months since they were notified of this action. Accordingly, Plaintiffs are entitled to an entry of default.

Upon the Court's entry of default pursuant to this request, Plaintiffs intend, thereafter, to file a motion for default judgment and permanent injunction pursuant to Fed. R. Civ. P. 55(b)(2) and Local Civil Rule 55.2(b), transferring the malicious domains in suit to Microsoft and enjoining Defendants from the conduct complained of in this action.

I. STATEMENT OF FACTS

A. Procedural History

Plaintiffs filed this suit on March 19, 2012, alleging that Defendants controlled a large number of Internet domains, as the "command and control" infrastructure for the Zeus

[1] Plaintiffs do not at this time move for default as to Defendants Yevhen Kulibaba (John Doe 22) or Yuriy Konovalenko (John Does 23/24). Plaintiffs have voluntarily dismissed John Doe 36. *See* DI 30.

botnets. Plaintiffs alleged that the pernicious effects of the botnets caused and continued to cause irreparable injury to Plaintiffs, their customers and members and the public, and stated claims for: (1) violation of the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) violation of the CAN-SPAM Act (15 U.S.C. § 7704); (3) violation 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) violation of the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962(c)); (8) unjust enrichment; (9) trespass to chattels; and (10) common law conversion.

Simultaneously, Plaintiffs applied *ex parte* for an Emergency Temporary Restraining Order and preliminary injunction to disable the Zeus botnets command and control server software, operating from and through the domains at issue in this case. The Court issued an *Ex Parte* Temporary Restraining Order, Seizure Order and Order to Show Cause Re Preliminary Injunction ("the TRO") on March 19, 2012. The order was executed on March 23, 2012 – all of the domains were disabled, and Defendants' software operating at and through these domains was, thus, disabled. On March 29, 2012, the Court issued a Preliminary Injunction disabling, during the pendency of this action, the domains through which the Defendants operated and controlled the Zeus botnets.

When it issued the TRO and Preliminary Injunction, the Court found good cause to permit service of Plaintiffs' Complaint and related materials by alternative means pursuant to Rule 4(f)(3). The Court has directed that, under the circumstances, appropriate means of service authorized by law, satisfying Due Process, and reasonably calculated to notify Defendants of this action, included transmission by electronic messaging and e-mail and other contact information associated with Defendants or provided by Defendants to domain registrars and Internet hosting providers who provided services that were used by Defendants to host the Zeus command and control infrastructure and publication of notice of these proceedings on a publicly available Internet website. The Court further granted

Plaintiffs the ability to serve discovery, in order to obtain further contact and identifying information regarding Defendants.

B. Investigation Regarding Defendants' Contact And Identifying Information

Through the discovery process and informal discovery efforts, Plaintiffs have gathered further contact information—particularly email addresses—at which to serve Defendants. Declaration of Gabriel M. Ramsey ("Ramsey Decl."), ¶¶ 6-48, filed herewith.

However, given (a) Defendants' uses of aliases and false information, (b) limitations in the ability to carry out non-U.S. discovery, (c) the ease with which anonymous activities can be carried out through the Internet and (d) the sophistication of the Defendants, Microsoft has been unable to specifically and definitively determine the "real" names and physical addresses of Defendants, at which they might be formally served by personal delivery or treaty-based means. Ramsey Decl., ¶ 8. Notwithstanding these limitations, the investigation has yielded additional email addresses associated with the Defendants and with the domains used to control the Zeus botnets. *Id.*, ¶¶ 8-9, 12. It is Plaintiffs' position that service of process directed to all such contact information associated with the Zeus botnets control servers and domains should be found to convey notice to the party or parties responsible for the botnets.

C. Service of the Complaint on Defendants

As soon as the TRO was executed on March 23, 2012, Plaintiffs undertook extraordinary efforts to serve Defendants with the Complaint, Amended Complaint, summons and related materials using the Court-ordered methods of service. Ramsey Decl., ¶¶ 10-48. The following sets forth Plaintiffs' service of the Complaint, Amended Complaint summons and pleadings in this case.

1. Service By Email

Between March 24, 2011 and June 30, 2011, Plaintiffs served by email copies of the Complaint, Amended Complaint each summons and all orders and pleadings in this action

by (1) emailing them to each email address or messaging address known to be associated with Defendants from independent investigation prior to the case, (2) emailing them to each email address used by Defendants to sign up for the Zeus botnet domains at issue and (3) emailing them to each further email address developed during discovery associated with Defendants and the Zeus botnet domains. Ramsey Decl., ¶¶ 12-48. Through this effort, the Defendants have been served at over 2,700 email and messaging addresses. Demonstrating that this method of service was effective, several of the Defendants responded to Plaintiffs making indications that they did not intend to appear or demanding that Plaintiffs cease communications with them. *See* Ramsey Decl., ¶¶ 16, 31. Despite this robust notice and service, the Defendants have not come forward in this action to defend or seek reinstatement of the Zeus botnet domains.[2]

2. Service By Internet Publication

Beginning on March 24, 2012, Plaintiffs published the Complaint, copies of each summons and all orders and pleadings in this action on the publicly available website www.zeuslegalnotice.com. The Amended Complaint and all subsequent pleadings and orders have been made available on that website throughout the case. The Court-approved notice language was provided in Russian, Ukrainian, Romanian and English on this website. A link to the website and the approved notice language was sent in each service of process email and messaging communication sent to Defendants at the over 2,700 email and messaging addresses to which service was effected. Ramsey Decl., ¶¶ 11.

---

[2] Plaintiffs investigated notice and service to facsimile numbers and mailing addresses contained in the records with respect to the domains at issue. This information appears to have been falsified. For example, Plaintiffs have verified many instances in which the name and address information used to register domains had been stolen from victims whose credentials had been stolen by Defendants and used to purchase the domains for illicit purposes. It is likely that Defendants used the Zeus software to steal these credentials. Plaintiffs' counsel communicated directly with a number of such victims, who confirmed that the names and addresses used to purchase botnet domains were their own. Some confirmed that their accounts had been used to purchase such domains. In each such instance, however, the victims confirmed that none of the email addresses used to register the domains were the victims' actual email addresses. Rather, these email addresses associated with the domains and to which service of processes was effected were associated solely with Defendants and are the most viable way to communicate with the Defendants in this action. Ramsey Decl., ¶¶ 47-48.

3. Defendants Are Likely Aware Of This Proceeding Given The Impact Of The TRO And Preliminary Injunction

Defendants very likely are aware of these proceedings, as the Court's TRO and Preliminary Injunction dealt a serious blow to the Zeus botnets. Because the IP addresses and domains controlling the botnets have been disabled since March 23, Defendants have not been able to access their software which was operating through those IP addresses and domains, and have not been able to communicate with Zeus-infected end-user machines using those IP addresses and domains. This has impeded these Zeus botnets' ability to grow and significantly disrupted the ability to steal credentials. Ramsey Decl., ¶ 10. Based on control of the botnet domains during the pendency of the case, Microsoft has discovered that the number of detected infected computers in this group of botnets has dropped from 779,816 as of March 25, to 336,393 as of June 17. *Id.* Since the issuance of the TRO and preliminary injunction, NACHA's measurement of spam email infringing the NACHA trademarks reveals that such activity has dropped by 90%. *Id.* This could hardly have escaped Defendants' attention. Third-party observers of the Zeus botnet have widely reported about this action, and Defendants are likewise also very likely to be aware of the impact on the botnet and to be aware that the instant proceeding is the cause of that impact. *Id.*

II. THE COURT SHOULD ENTER DEFAULT UNDER FED. R. CIV. P. 55(A) BECAUSE THE DEFENDANTS – DESPITE HAVING BEEN SERVED – HAVE FAILED TO ANSWER OR OTHERWISE APPEAR

Under Fed. R. Civ. P. 55(a) "when a party against whom a judgment for affirmative relief is sought has failed to plead or otherwise defend, and that failure is shown by affidavit or otherwise, the clerk must enter the party's default." Between March 24, 2012 and present, Plaintiffs served the Complaint, Amended Complaint, summons and all orders and pleadings on Defendants using the methods ordered by the Court under Rule 4(f)(3), including service by email and publication. These methods of service satisfy Due Process and were reasonably calculated to notify the Defendants of this action.

Courts have come to appreciate the need to resort to alternative means of serving evasive international defendants, whose physical address is unknown. The Ninth Circuit in *Rio Props., Inc. v. Rio Int'l Interlink*, for example, recognized that service by email is particularly warranted in cases – such as this one – involving Internet-based misconduct perpetrated by international defendants, as perhaps the only method "aimed directly and instantly" at serving international e-business defendants:

> [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 email-the method of communication which [Defendant] utilizes and prefers. In addition, email was the only court-ordered method of service aimed directly and instantly at [Defendant] … Indeed, when faced with an international e-business scofflaw, playing hide-and-seek with the federal court, email may be the only means of effecting service of process.

Rio Props., Inc. v. Rio Int'l Interlink, 284 F.3d 1007, 1014-15 (9th Cir. 2002). Since *Rio Props.*, several courts have found email an appropriate alternative means of service under Rule 4(f)(3) in cases involving online malfeasance by international defendants. *See e.g.*, *Gurung v. Malhotra*, 279 F.R.D. 215, 220 (S.D.N.Y. 2011) (finding service by email effective under Rule 4(f)(3)); *Prediction Co. LLC v. Rajgarhia*, 2010 U.S. Dist. LEXIS 26536 (S.D.N.Y. Mar. 22, 2010) (same); *Williams-Sonoma, Inc. v. Friendfinder, Inc.*, 2007 U.S. Dist. LEXIS 31299, *5-6 (N.D. Cal. Dec. 6, 2007) (finding service by email consistent with the Hague Convention and warranted in cases involving misuse of Internet technology by international defendants); *Liberty Media Holdings, LLC v. Vinigay.com*, 2011 U.S. Dist. LEXIS 26657, *11 (D. Ariz. March 3, 2011) (finding service by email appropriate on Brazilian defendants who had downloaded copyrighted material off the Internet); *Liberty Media Holdings, LLC v. March*, 2011 U.S. Dist. LEXIS 5290, *4-5 (S.D. Cal. Jan. 20, 2011) (finding service by email appropriate on foreign defendants who had registered Internet domain names that allegedly infringed plaintiff's trademarks); *see also FMAC Loan Receivables v. Dagra*, 228 F.R.D. 531, 534 (E.D. Va. 2005) (acknowledging that courts have readily used Rule 4(f)(3) to authorize international service through non-traditional means,

including email).

As discussed, Plaintiffs successfully sent thousands of emails and electronic messages containing or linking to the Complaint, Amended Complaint, Summons and the orders and pleadings in this proceeding to the email and messaging addresses associated with the Defendants and their Zeus botnet domains, or otherwise discovered in this case as being associated with Defendants. Ramsey Decl., ¶¶ 11-46. Given that Defendants' preferred mode of communication regarding the botnet servers was electronic means, as evidenced by their use of stolen information to sign up for the domains *except for email addresses* which were actually associated with Defendants (*Id.* ¶ 47), given the direct association between the email addresses and the botnet infrastructure, and given that the pleadings were successfully sent to thousands of such addresses, it is appropriate to find that the Complaint, Amended Complaint and summons were served on Defendants pursuant to *Rio Props.* and other authority approving email as a valid means of service.

Federal Courts have also routinely authorized service on international defendants by publication when it is reasonable to conclude that the defendants are likely to read the media in which the notice is published. *See BP Prods. N. Am., Inc. v. Dagra*, 236 F.R.D. 270, 271-273 (E.D. Va. 2005) (approving notice by publication in two Pakistani newspapers circulated in the defendant's last-known location); *Smith v. Islamic Emirate of Afghanistan,* 2001 U.S. Dist. LEXIS 21712 (S.D.N.Y. Dec. 26, 2001) (approving service by publication upon Osama bin Laden and the al-Qaeda organization); *SEC v. HGI, Inc.*, 1999 U.S. Dist. LEXIS 17441, *4-5 (S.D.N.Y. Nov. 5, 1999) (approving service by publication in a national newspaper); *Morris v. Khadr*, 415 F. Supp. 3d 1323, 1327 (D. Utah 2006) (allowing the plaintiffs to serve defendant in Toronto by publishing notice in a newspaper and posting the complaint on a website "www.september11classaction.com").

Here, while Defendants' specific physical addresses are unknown, the evidence indicates that Defendants carry out business through the email and messaging addresses to which service was effected and to which the pleadings and links to

www.zeuslegalnotice.com were sent. Accordingly, notice of the instant proceedings by publication through the www.zeuslegalnotice.com website is appropriate.[3] Given that the links were provided in emails to Defendants' primary mode of communication and that the website and emails contained notice language in Russian, Ukrainian, Romanian and English, they are likely to be read by Defendants and likely to apprise Defendants of this action.

All of the above-mentioned methods of service advised Defendants of the nature of this action and the relief sought, directed Defendants how to respond to the Complaint, provided contact information to do so and provided a link to the website www.zeuslegalnotice.com, where all documents in the case have been published. This publicly available website has been continuously available and has contained all documents in the case since March 24, 2012. *Id.*, ¶ 11. Several of the Defendants have responded to electronic communications that included the website link, but have indicated that they did not intend to appear. *Id.* ¶¶ 16, 31. Other interested members of the public have inquired about the website notices. *Id.* ¶ 11. These facts indicate that these communications and the service of process website are in fact reaching the public and the Defendants, and are an effective means to cause interested parties, including the Defendants, to respond if they wish to do so. Given these facts, it is appropriate to find that the Complaint, Amended Complaint and summons were served on Defendants pursuant to authority approving publication as valid means of service.

Further, Defendants are almost certainly aware of the action because of the dramatic effect the Court's TRO and preliminary injunction has had on this group of Zeus botnets and the widespread and detailed coverage of this action in media across the world. *Id.* ¶ 10. Accordingly, it is very likely that Defendants are likewise aware of these proceedings.

Thus, for all of the foregoing reasons, the Complaint, Amended Complaint and

---

[3] Given that Defendants' specific addresses are unknown, the Hague Convention does 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 Products North 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.")

summons should be deemed served upon John Doe Defendants 1-21, 25-35, 37-39 for a period of greater than 21 days. Despite Plaintiffs' extraordinary efforts to serve Defendants and provide them with notice of the action, they have failed to plead or otherwise defend against the action. Given the Defendants' sophisticated activities and all other information known about them, there is no evidence indicating that they are infants, in the military or incompetent persons. Ramsey Decl., ¶ 7. Therefore, pursuant to Fed. R. Civ. P. 55(a) and Local Civil Rule 55.1, entry of default against the non-responsive Defendants is appropriate. *See Gurung v. Malhotra*, 279 F.R.D. 215, 220 (S.D.N.Y. 2011) (entering default against non-responsive international defendant served by email); *Prediction Co. LLC v. Rajgarhia*, 2010 U.S. Dist. LEXIS 26536 (S.D.N.Y. Mar. 22, 2010) (same); *Gucci Am. v. Huoqing*, 2011 U.S. Dist. LEXIS 776 (N.D. Cal. 2011) (default entered against defendant based on identity contained in domain WHOIS information associated with domain through which counterfeit Gucci bags were sold); *Transamerica Corp. v. Moniker Online Servs., LLC.*, 2010 U.S. Dist. LEXIS 48016 (S.D. Fl. 2010) (default entered against fictitious individual who had used a false name and fake address in registering and using internet domain names infringing trademark).

III. CONCLUSION

For all of the foregoing reasons, entry of default against the John Doe Defendants 1-21, 25-35, 37-39 is appropriate. Plaintiffs respectfully request entry of default against these non-responsive Defendants.

Dated: August 2, 2012
New York, New York

Respectfully Submitted,

ORRICK, HERRINGTON & SUTCLIFFE LLP

By: _____
Richard A. Jacobsen
51 West 52nd Street
New York, NY 10019
Telephone: (212) 506-5000

Facsimile: (212) 506-5151

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