IN THE UNITED STATES DISTRICT COURT

FOR THE WESTERN DISTRICT OF NORTH CAROLINA

CHARLOTTE DIVISION

MICROSOFT CORPORATION, Plaintiff, v. JOHN DOES 1-82, CONTROLLING A COMPUTER BOTNET THEREBY INJURING MICROSOFT AND ITS CUSTOMERS, Defendant.	Civil Action No. 3:13-CV-00319-GCM **MOTION FOR ENTRY OF DEFAULT**

Plaintiff Microsoft Corp. ("Microsoft" or "Plaintiff") respectfully requests, pursuant to Fed. R. Civ. P. 55(a), that the Court enter default against Defendants John Doe 1-82 ("Defendants") who operated and controlled the Citadel botnets from and through the Internet domains at issue in this case. Entry of default is warranted here. Plaintiff served Defendants with the 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 with the opportunity to respond. Plaintiff 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, Plaintiff is entitled to an entry of default.

Upon the Court's entry of default pursuant to this request, Plaintiff intends, thereafter, to file a motion for default judgment and permanent injunction pursuant to Fed. R. Civ. P. 55(b)(2), 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

Plaintiff filed this suit on May 29, 2013, alleging that Defendants controlled a large number of Internet domains, as the "command and control" infrastructure for the Citadel botnets. Plaintiff alleged that the deleterious effects of the botnets caused and continued to cause irreparable injury to Plaintiff, its customers and members of the public, and stated claims for violation of the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the CAN-SPAM Act (15 U.S.C. § 7704); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq*.); the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); North Carolina General Statute § 14-458 (Computer Trespass); and the common law of conversion, unjust enrichment, and nuisance. Plaintiff has also moved for a preliminary injunction under Fed. R. Civ. P. 65(b), 15 U.S.C. § 1116(d) (the "Lanham Act") and 28 U.S.C. § 1651(a) (the "All Writs Act"), and an order to show cause why a preliminary injunction should not be granted.

Simultaneously, Plaintiff applied *ex parte* for an Emergency Temporary Restraining

Order and preliminary injunction to disable the Citadel 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 May 29, 2013. The order was executed on June 5, 2013 – all of the domains were disabled, and Defendants' software operating at and through these domains was, thus, disabled. On June 11, 2013, the Court issued a Preliminary Injunction disabling, during the pendency of this action, the domains through which the Defendants operated and controlled the Citadel botnets.

When it issued the TRO and Preliminary Injunction, the Court found good cause to permit service of Plaintiff's 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 Citadel command and control infrastructure and publication of notice of these proceedings on a publicly available Internet website. The Court further granted Plaintiff the ability to pursue 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, Plaintiff has gathered further contact information – particularly email addresses – at which to serve Defendants. Declaration of James M. Hsiao in Support of Microsoft's Motion for Entry of Default ("Hsiao Decl."), ¶ 6.

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. Hsiao Decl., ¶ 8. Based on our current discovery responses and investigation, Plaintiff believes that further discovery will not result any additional actionable information that may be reasonably calculated to reveal Defendants' identities and, thus, is likely futile. It is Plaintiff's position that service of process directed to all contact information associated with the Citadel botnets command and 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 June 5, 2013, Plaintiff undertook extraordinary efforts to serve Defendants with the Complaint, summons, and related materials using the Court-ordered methods of service. Declaration of Gabriel M. Ramsey in Support of Microsoft's Motion for Entry of Default ("Ramsey Decl."), ¶ 2 & Hsiao Decl., ¶¶ 11-15. The following sets forth Plaintiff's service of the Complaint, summons and pleadings in this case.

1. Service By Email

Plaintiffs served by email copies of the Complaint, 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 and (2) emailing them to each email address used by Defendants to sign up for the Citadel botnet domains at issue. Hsiao Decl., ¶¶ 12-13. Through this effort, the Defendants have been served by over

2,900 emails and messaging communications. Demonstrating that this method of service was effective, at least one Defendant—John Doe 1, the ultimate creator and distributor of the Citadel botnet software—has contacted Plaintiff through one of these messaging addresses, and after being notified regarding the Complaint and pending suit, has since ceased communication. Ramsey Decl., ¶¶ 2-7. Despite this robust notice and service, the Defendants have not come forward in this action to defend or seek reinstatement of the Citadel botnet domains.[1]

2. Service By Internet Publication

Beginning on June 5, 2013, Plaintiff published the Complaint, copies of each summons, and all orders and pleadings in this action on the publicly available website www.botnetlegalnotice.com/citadel. The notice language was provided in Russian and English on this website. A link to the website and the notice language was sent in each service of process email and messaging communication sent to Defendants via over 2,900 emails and messaging communications to which service was effected. Hsiao Decl., ¶ 11.

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

Defendants are very likely aware of these proceedings, as the Court's TRO and Preliminary Injunction dealt a serious blow to the Citadel botnets. Because the IP addresses and domains controlling the botnets have been disabled since June 5, 2013, 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 Citadel-infested end-user machines using those IP

[1] Plaintiff investigated notice and service to facsimile numbers and mailing addresses contained the records of the domain registrars with respect to the domains at issue. This information appears to have been falsified. For example, Plaintiff have verified 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. The email addresses associated with the domains and to which service of processes was effected are the only information from the records that are likely to be actually associated with Defendants and are the most viable way to communicate with the Defendants in this action. Hsiao Decl., ¶ 15.

addresses and domains. This has impeded these Citadel botnets' ability to grow and significantly disrupted the ability to steal credentials. Hsiao Decl., ¶ 10. Based on control of the botnet domains during the pendency of the case, Microsoft has discovered that over 2.1 million infected computers have been removed from the Citadel botnets after the execution of the TRO. *Id.* It would be impossible for this to have escaped Defendants' attention. This action has been widely reported by a number of third-parties as the cause of that impact, and thus, Defendants are likely 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 June 5, 2013 and present, Plaintiff served the 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. Furthermore, these methods of service are means of service authorized by the Court in its Order at Docket No. 15 and is authorized pursuant to Fed. R. Civ. P. 4(f).

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.*, a number of courts, including other district courts in the Fourth Circuit, 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., Microsoft Corp. v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va. 2010, Brinkema J.) at Dkt. 38, p. 4 (authorizing notice of preliminary injunction and service on botnet operators by e-mail, facsimile, mail and publication); *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); *see also Gurung v. Malhotra*, 279 F.R.D. 215, 220 (S.D.N.Y. 2011) (finding service by email effective under Rule 4(f)(3)); *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); *Prediction Co. LLC v. Rajgarhia*, 2010 U.S. Dist. LEXIS 26536 (S.D.N.Y. Mar. 22, 2010) (finding service by email effective under Rule 4(f)(3)); *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).

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 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"); *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).

As explained above, Plaintiff successfully sent thousands of emails and electronic messages containing or linking to the Complaint, summons and all the orders and pleadings in this proceeding to the email and messaging addresses associated with the Defendants and their Citadel botnet domains. Hsiao Decl., ¶¶ 11-14. Given that Defendants' preferred mode of communication regarding the botnet servers was via electronic means, as evidenced by a defendant contacting Plaintiff's counsel electronically and was given personal notice regarding this action (Ramsey Decl., ¶¶ 2-7), 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 and summons were served on Defendants pursuant to this Court's order, *Rio Props.*, and other authority approving email as a valid means of service.

Furthermore, 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.botnetlegalnotice.com/citadel were sent. Accordingly, notice of the instant proceedings by publication through the ww.botnetlegalnotice.com website is appropriate.[2] 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 and English, they are likely to be read by Defendants and likely to apprise Defendants of this action.

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

Thus, for all of the foregoing reasons, the Complaint and summons should be deemed served upon John Doe Defendants 1-82 for a period of greater than 21 days. Despite Plaintiff's 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. Hsiao Decl., ¶ 7. Therefore, pursuant to Fed. R. Civ. P. 55(a), entry of default against the non-responsive Defendants is appropriate here. *See 3M Co. v. Christian Invs. LLC,* 2012 U.S. Dist. LEXIS 64104, *4 (E.D. Va. 2012) (default entered against non-responsive international defendant served pursuant to Rule 4(f)); *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.

[2] 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.")

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 1-82 is appropriate. Microsoft respectfully requests entry of default against these non-responsive Defendants.

Dated: October 21, 2013

By: s/Neil T. Bloomfield

Neil T. Bloomfield
NC Bar No. 37800

Moore & Van Allen PLLC
100 North Tryon Street
Suite 4700
Charlotte, NC 28202-4003
Telephone: +1-704-331-1084
Facsimile: +1-704-409-5660
Email: neilbloomfield@mvalaw.com

Of counsel:

Gabriel M. Ramsey (*pro hac vice*)
Orrick, Herrington & Sutcliffe LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401
Email: gramsey@orrick.com

Jeffrey L. Cox (*pro hac vice*)
Orrick, Herrington & Sutcliffe LLP
701 5th Avenue, Suite 5600
Seattle, WA 98104-7097
Telephone: (206) 839-4300
Facsimile: (206) 839-4301
Email: jcox@orrick.com

James M. Hsiao (*pro hac vice*)
Orrick, Herrington & Sutcliffe LLP
777 South Figueroa Street
Suite 3200
Los Angeles, CA 90017-5855
Telephone: (213) 612-2449
Facsimile: (213) 612-2499
Email: jhsiao@orrick.com

Attorneys for Plaintiff