



## **I. STATEMENT OF FACTS**

This action arises out of violations of federal and state law caused by John Doe Defendants' operation of a malicious computer botnet known as the "Shylock" botnet. Defendants are the persons responsible for operating IP addresses and Internet domains used to propagate and control the Shylock botnet. On June 27, 2014, the Court entered a TRO that disabled much of the Shylock botnet's command and control infrastructure. Dkt. 16. The Court subsequently entered a Preliminary Injunction to ensure that Defendants' malicious infrastructure cannot be used to cause further harm pending final resolution of this case. Dkt. 33.

When the Court 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). Dkt. 16 at 7. The Court has directed that, under the circumstances, appropriate means of service sufficient to satisfy Due Process include emails to email accounts associated with Defendants and publication on a publically available Internet website. *Id.*

The Court further granted Plaintiffs the ability to pursue discovery, in order to obtain further contact and identifying information regarding Defendants. Doe discovery is now complete. Dkt. 47. Because Defendants used fake contact information and stolen credit card numbers to set up these IP addresses and Internet domains, Defendants' true identities remain unknown. Declaration of Jacob M. Heath ("Heath Decl.") ¶¶ 4, 6.

### **Plaintiffs' Doe Discovery Efforts**

Over the past six months, Plaintiffs have issued subpoenas to domain registrars, hosting companies, email providers, and other Internet service providers ("collectively ISPs") in an effort to obtain additional information regarding Defendants' identities. Heath Decl. ¶¶ 2, 3. Plaintiffs issued a first wave of subpoenas shortly after execution of the Court's Temporary Restraining Order. Heath Decl. ¶ 4. Based on information obtained during Plaintiffs' first wave of doe discovery, Plaintiffs sent subpoenas and informal discovery requests to additional ISPs. Heath Decl. ¶ 4. Plaintiffs also conducted telephone interviews with persons of interest. Heath Decl. ¶ 5.

Plaintiffs' due discovery efforts yielded several names, addresses, and email addresses that were previously unknown to Plaintiffs, as well as various credit card account numbers used to pay for services associated with the Shylock botnet. Heath Decl. ¶ 4. Further investigation revealed that the names, addresses, and credit card information used by Defendants were fake or stolen. Heath Decl. ¶ 4.

Plaintiffs identified six individuals residing abroad who have been associated with infrastructure for the Shylock botnet over the past year. Heath Decl. ¶ 5. Plaintiffs interviewed two of these individuals via telephone and they stated that they did not have possession or control of the relevant infrastructure during the relevant time period. Heath Decl. ¶ 5. These two individuals provided documentary evidence supporting their statements. Heath Decl. ¶ 5. Plaintiffs have been unable to speak with the other four individuals identified, three of whom appear to be hosting service resellers. Heath Decl. ¶ 5. Because these individuals are located beyond the Court's subpoena power in non-Hague Convention jurisdictions, and because these individuals are not cooperating with Plaintiffs' attempts to obtain information informally, Plaintiffs' investigation regarding these individuals and their ties to Defendants has reached a dead end. Heath Decl. ¶¶ 5, 6.

Plaintiffs have exhausted their ability to investigate Defendants' true identities using civil discovery tools, despite their best efforts and the exercise of reasonable diligence to determine Defendants' identities. Heath Decl. ¶ 6.

### **Service of Process on Defendants**

The Court authorized service by email and publication on June 27, 2014. On July 14, 2014, after the case was unsealed, Plaintiffs served email addresses associated with Defendants' IP addresses and Internet domains. Heath Decl. ¶ 7. Plaintiffs also served defendants by publication at July 8, 2014 at the website <http://botnetlegalnotice.com/shylock/>. Heath Decl. ¶ 8. Plaintiffs used an email tracking service to monitor whether service emails were received and read. Heath Decl. ¶ 7. The vast majority of service emails were undeliverable, apparently because the email addresses were fake or had been closed. Heath Decl. ¶ 7.

During the course of due discovery, Plaintiffs identified 15 additional email addresses of interest associated with Shylock botnet infrastructure. Heath Decl. ¶ 9. These emails consist of recovery emails associated with previously identified email addresses and alternative email contact for domains and IP addresses associated with the Shylock botnet. Heath Decl. ¶ 9. On January 8, 2015, Plaintiffs served these additional email addresses and also re-served the functioning email addresses previously served during the first wave of service. Heath Decl. ¶ 11.

The time for Defendants to answer or respond to the complaint expired 21 days after service of the summons—at the latest, on August 4, 2014 (21 days after email service). Heath Decl. ¶ 13. To the best of Plaintiffs' information and belief, no Defendant is a minor or incompetent person. Heath Decl. ¶ 13.

## **II. LEGAL AUTHORITY**

“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.” Fed. R. Civ. P. 55(a). Plaintiffs have 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, particularly given the nature of Defendants' conduct. *See, e.g., 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); *Rio Props., Inc. v. Rio Int'l Interlink*, 284 F.3d 1007, 1014-15 (9th Cir. 2002) (“[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...”); *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); *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 service by email and publication in similar action).

As explained above, Plaintiff successfully sent numerous service emails to the email addresses associated with the Defendants and their Shylock botnet domains. Heath Decl., ¶¶ 11, 12. Given that Defendants' preferred mode of communication regarding the botnet servers was via electronic means, 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. Heath Decl., ¶ 9. While Defendants' specific physical addresses are unknown, the evidence indicates that Defendants carry out business through the email addresses. Heath Decl., ¶ 9. Moreover, it is likely that Defendants are aware of the notice website, which has been publically available since July 8, 2014 and is the very first Google hit for the search "shylock botnet notice." Heath Decl., ¶ 8. Defendants are undoubtedly aware that they have lost control of much of the Shylock botnet infrastructure, and any cursory investigation would reveal that Plaintiffs have initiated this lawsuit, which has been discussed by online news outlets. Heath Decl., ¶ 13.

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)).

### **III. CONCLUSION**

For all of the foregoing reasons, entry of default against the John Doe Defendants 1-8 is appropriate. Plaintiffs respectfully request entry of default pursuant to Rule 55(a) so that Plaintiff can proceed with a motion for default judgment.

Dated: January 22, 2015

Respectfully submitted,

ORRICK, HERRINGTON & SUTCLIFFE LLP

/s/ Lauren J. Parker

LAUREN J. PARKER

Va. State Bar No. 77018

Attorneys for Plaintiffs Microsoft Corp. and FS-ISAC, Inc.

ORRICK, HERRINGTON & SUTCLIFFE LLP

Columbia Center

1152 15th Street, N.W.

Washington, D.C. 20005-1706

Telephone: (202) 339-8400

Facsimile: (202) 339-8500

lparker@orrick.com

Of counsel:

GABRIEL M. RAMSEY (admitted *pro hac vice*)

JACOB M. HEATH (admitted *pro hac vice*)

ROBERT URIARTE (admitted *pro hac vice*)

Attorneys for Plaintiffs Microsoft Corp. and FS-ISAC, Inc.

ORRICK, HERRINGTON & SUTCLIFFE LLP

1000 Marsh Road

Menlo Park, CA 94025

Telephone: (650) 614-7400

Facsimile: (650) 614-7401

gramsey@orrick.com

jheath@orrick.com

ruriarte@orrick.com