IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

MICROSOFT CORPORATION, a Washington corporation, and FS-ISAC, INC., a Delaware corporation, Plaintiffs, v. JOHN DOES 1-8, CONTROLLING A COMPUTER BOTNET THEREBY INJURING PLAINTIFFS, AND THEIR CUSTOMERS AND MEMBERS, Defendants.	Civil Action No: 1:14-cv-811 LOG/TCB

DECLARATION OF JACOB M. HEATH
IN SUPPORT OF PLAINTIFFS' REQUEST FOR DEFAULT

I, Jacob M. Heath, declare as follows:

1. I am an attorney with the law firm of Orrick, Herrington & Sutcliffe LLP ("Orrick"), counsel of record for Plaintiffs Microsoft Corporation ("Microsoft") and Financial Services-Information Sharing and Analysis Center, Inc. ("FS-ISAC") (collectively "Plaintiffs"). I make this declaration in support of Plaintiffs' Application for default. I make this declaration of my own personal knowledge and, if called as a witness, I could and would testify competently to the truth of the matters set forth herein.

Doe Discovery

2. I am one of the attorneys primarily responsible for conducting doe discovery and investigating facts related to Defendants' identities. Over the past six months, Plaintiffs have issued approximately twenty subpoenas to third party registrars, web hosting services, email service providers, and other Internet Service Providers ("ISPs"). Plaintiffs have also conducted interviews and engaged in correspondence with persons in the United States and abroad in an attempt to locate

information sufficient to identify and personally serve John Does 1-8.

3. Based on information in Plaintiffs' possession regarding the infrastructure that John Does 1-8 have used to operate the Shylock botnet, my firm has issued subpoenas to the following entities since entry of the Court's order permitting doe discovery: Bizcn.com, Inc.; ColoCrossing; Gandi SAS; Google, Inc.; Hosting Solutions International, Inc.; Moniker Online Services LLC; Network Solutions LLC; PakNIC Private Limited; PDR Ltd.; Register.com; Spirit Communication Corp.; Tucows, Inc.; Web Commerce Communications Limited; Webfusion Internet Solutions, Inc.; and Enom, Inc.

4. Multiple subpoenants have provided information such as IP addresses, email addresses, names, physical addresses, payment information, and dates of use for infrastructure associated with the Shylock botnet. Plaintiffs followed up on these leads by issuing additional subpoenas, sending informal requests for information to ISPs who are beyond the Court's subpoena power, and by attempting to use the names and addresses obtained through doe discovery to attempt to contact Defendants. The names and credit card information used by Defendants to set up the Shylock botnet infrastructure appear to be false or stolen. For example, transaction records for various ISPs reflect fraud complaints and refunds issued to credit card holders whose accounts were used to register infrastructure related to the Shylock botnet.

5. During the course of our investigation, my office identified six natural persons associated with infrastructure related to the Shylock botnet. One of these persons appears to reside in Saudi Arabia, one appears to reside in Jakarta, Indonesia, one resides in Vietnam, two appear to reside in Russia, and one resides in Canada. The individuals in Vietnam and Canada participated in telephone interviews and stated that they did not control the Shylock infrastructure associated with them during the relevant time period. These individuals provided documentary evidence supporting their statements. In particular, the individual located in Canada hosted an online gaming server that is believed to have been used by the Defendants for purposes of the botnet at some point in time. The other of the individuals, in Vietnam, was a reseller of U.S.-based hosting services and is believed to have resold U.S.-based hosting to the Defendants. Neither of these individuals had information concerning the specific identities or contact information of the Defendants. The other

individuals did not respond to requests for interviews, however, a Russian company affiliated with the one of the persons we identified in Russia provided limited data to my office in response to an email inquiry. In particular, this company was a reseller of U.S.-based hosting resources, but indicated that it did not maintain information regarding its customer, such as name, physical address or payment information that could be attributed to any natural person or entity. The only information it could provide was an obscure nickname that was not attributable to any particular person and was insufficient to identify any Defendant. The Russian company ceased responding to our inquiries after the initial response. A second Russian entity that appears to be an internet service provider of some sort did not respond to our repeated email inquiries.

6. Despite diligent efforts, Plaintiffs are unable to ascertain Defendants' true identities, and Plaintiffs have exhausted their ability to investigate Defendants' identities using civil discovery tools. Plaintiffs cannot serve compulsory process on the individuals located in Indonesia, Saudi Arabia, or Russia, as the former two countries are not signatories to the Hague Convention on Service and Russia does not honor U.S. Hague Convention requests. *See* http://travel.state.gov/content/travel/english/legal-considerations/judicial/country/russia-federation.html ("In July 2003, Russia unilaterally suspended all judicial cooperation with the United States in civil and commercial matters. The Russian Federation refuses to serve letters of request from the United States").

Service of Process

7. The Court's June 27, 2014 Order (Dkt. 16) provides in pertinent part:

> There is good cause to permit notice of the instant Order…and service of the Complaint by formal and alternative means…the following means of service are authorized by law, satisfy Due Process, and satisfy Fed. R. Civ. P. 4(f)(3)…(3) transmission by email…(4) publishing notice on a publicly available Internet website

Accordingly, on July 14, 2014, my office served the Complaint, summons and all papers in this action to all email addresses known to be associated with the Shylock botnet. The complaint and summons were served both in the English and Russian languages. My office used the email tracking service ReadNotify to effect service. ReadNotify allows email senders to monitor when their email

is delivered, read, or forwarded and provides additional data in some instances (such as access IP address). According to ReadNotify, the majority of service emails "bounced;" i.e., the emails could not be delivered, apparently because the email addresses were fake or had been closed.

8. In addition to providing service by email, Plaintiffs also served Defendants by publication pursuant to the Court's June 27, 2014 order. On July 8, 2014, Plaintiffs posted a notice and copies of all pleading on the website: http://botnetlegalnotice.com/shylock/. The website has been continually online since July 8 and is the first Google search result for the search "shylock botnet notice." A link to this website was included in all of the service of process emails, along with the notice language (in both Russian and English), specified in the Court's June 27, 2014 Order.

9. During the course of doe discovery, Plaintiffs identified 15 additional email addresses of interest associated with Shylock botnet infrastructure and which were used by Defendants to register and maintain the botnet infrastructure. In particular, discovery obtained in the case indicated that Defendants would use fake and/or stolen identity and contact information and credit card information to purchase the botnet infrastructure. However, the email addresses used in the process of procuring this infrastructure was the single point of contact that Defendants actually used to communicate with the infrastructure providers and to consummate the purchase of the infrastructure. For this reason, I conclude that the email addresses are the only possible way to communicate with the Defendants.

10. Plaintiffs obtained email correspondence between ISPs and persons associated with Shylock IP address 192.3.20.89. Plaintiffs also obtained additional email addresses used in connection with Shylock domains Trendei.net, Bestmanta.net, Adestaventurez.com, Alphard-info.net, Isohotel.net, Nintendowiionline.net, Lanegovonline.net, Macdegredo.com, Paradigmcore.net, Micatoge.net, and Webercountyfairr.net. Plaintiffs also obtained recovery email addresses for Gmail accounts previously identified as email addresses for Defendants (a recovery email is an alternate email account used in setting up a Gmail account to facilitate password recovery, user authentication, etc.).

11. On January 8, 2015, my office re-served Defendants using the 15 newly uncovered

email addresses and the functioning email addresses previously served on July 15, 2014.

12. ReadNotify indicates that, as of the date of this declaration, at least 6 of the service emails were delivered, opened, and read. In particular, ReadNotify provides the following data:

Email Address	Service Email Open Date
awroemanto@gmail.com	1/9/2015 at 19:51
kankouni@gmail.com	1/19/2015 at 11:39
darkbluefirefly@gmail.com	1/12/2015 at 16:43
turpe@onbox.org	1/8/2015 at 16:57
cakesbyalicenl@priest.com	7/9/2014 at 4:21
c0d6195cf4dd49349a0793fd2aab4f62.protect@whoisguard.com	7/9/2014 at 4:03

13. The 21-day time for Defendants to respond to the complaint under Fed. R. Civ. P. 12 has expired, as Defendants were served on July 8, 2014 via publication and July 14, 2014 via email. On information and belief based on Plaintiffs investigation, and the sophistication of the operation of the botnet and the procurement of infrastructure to operate the botnet, no Defendant is a minor or incompetent person, and each Defendant is likely to have notice of these proceedings by virtue of disruption to the Shylock botnet caused by the TRO and coverage of this case by multiple online news outlets.

I declare under penalty of perjury under the laws of the United States of America and the District of Columbia that the foregoing is true and correct to the best of my knowledge.

Executed this, the 22nd day of January, 2015 in Menlo Park, California.

Jacob M. Heath