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, Defendants.	Civil Action No. 3:13-CV-00319-GCM **DECLARATION OF JAMES M. HSIAO IN SUPPORT OF MOTION FOR ENTRY OF DEFAULT**

I, James M. Hsiao, declare as follows:

1. I am an associate of the law firm of Orrick, Herrington & Sutcliffe LLP ("Orrick"), counsel of record for Plaintiff Microsoft Corp. ("Microsoft" or "Plaintiff"). I make this declaration in support of Microsoft's Motion for Entry of 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.

I. DEFENDANTS HAVE NOT RESPONDED OR OTHERWISE REQUESTED THAT THE DOMAINS AT ISSUE IN THIS CASE BE REINSTATED.

2. On June 5, 2013, Plaintiff's counsel at Orrick served copies of the Complaint, TRO and all associated pleadings to the U.S. domain registries which have control over the Internet namespace associated with the Citadel botnet command and control domains. Subsequently, on June 11, 2013, the registries were served with the Preliminary Injunction. These documents were also delivered to the attention of non-U.S. domain registries, with an

informal request for their assistance in preventing Defendants from accessing the command and control domains.

3. Since that time, Plaintiff's counsel at Orrick, Herrington & Sutcliffe have been in continuous contact with the foregoing domain registries. The domain registries, and the ultimate domain registrars which sold the domains to the defendants, were provided with Plaintiff's counsel's information. These parties were asked to inform Plaintiff's counsel if any of the Defendants requested reinstatement of the domains and were asked to have Defendants contact Plaintiff's counsel about the case if any communication was received from them.

4. As of October 18, 2013, Plaintiff's counsel has received no request from any of the Defendants to reinstate the command and control domains.

5. As described more fully below, John Doe Defendants 1-82 have been properly served the Complaint and summons in this matter pursuant to the means authorized in the Court's temporary restraining order and preliminary injunction, and these Defendants have failed to plead or otherwise defend the action.

II. INVESTIGATION REGARDING DEFENDANTS' CONTACT AND IDENTIFYING INFORMATION.

6. Through the discovery process and informal discovery efforts, Plaintiffs have gathered further contact information—particularly email addresses—at which to serve Defendants.

7. Based upon their operation of a sophisticated group of botnets, previously available information and information developed in discovery, upon information and belief, the Defendants are not infants, in the military or incompetent persons.

8. Given (a) Defendants' usage 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, we have been unable to specifically and definitively determine the "real" names and physical addresses of Defendants, at which they might be served by personal delivery or treaty-based means.

9. Notwithstanding these limitations, Plaintiff has been able to locate multiple pieces of contact information, particularly email addresses associated with the domains at issue in this case and email and messaging addresses otherwise associated with the Defendants. 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 will convey notice to the parties responsible for the Citadel botnets.

III. SERVICE OF PROCESS AND NOTICE UPON DEFENDANTS

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

10. The operation and growth of the Citadel botnets at issue in this case has been frustrated by the temporary restraining order and preliminary injunction issued by the Court. 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-infected end-user machines using those IP addresses and domains. This has impeded these Citadel botnets' ability to grow and significantly disrupted the ability to steal credentials. I am informed by Microsoft, based on control of the botnet domains during the pendency of the case, that over 2.1 million detected Citadel-infected computers have been removed from Citadel botnets since the execution of the temporary restraining order. This action has been widely reported by a number of third-parties and I have confirmed that the action has been reported in public media, including multiple European countries, Russia, and the United States. Given the obvious impact on the

botnets and public reports of this action, Defendants are likely to be aware of Microsoft's successful disruption and mitigation efforts and to be aware that the instant proceeding is the cause of that impact.

2. Service By Internet Publication

11. 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 at the over 2,900 email and messaging addresses to which service was effected. Almost 8,000 unique visitors have visited the website between June 5 and September 30. Furthermore, Plaintiff's counsel have been contacted by members of the public who have become aware of this case. Thus, I conclude that the website is effective at providing notice of this action and instructions on how to contact Plaintiff's counsel or otherwise respond.

3. Service By Email

12. Plaintiff served by email copies of the Complaint, summons, and a link to all pleadings in this action, as well as the notice language, through those means as described further below. Between the messaging and email addresses known to be associated with the Defendants and the email addresses associated with the botnet domains, the Defendants have been served by over 2,900 emails and messaging communications. 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.

13. **John Doe 1** ("aquabox") was served the notice language and link to www.botnetlegalnotice.com/citadel containing the Complaint, summons, and all documents in

this action, to the messaging address aquabox@jabber.org on June 5, 2013. John Doe 1 initiated communications with Plaintiff's counsel on August 2, 2013 from the aquabox@jabber.org address and indicated possession of and intent to sell the Citadel botnet software. *See* Declaration of Gabriel M. Ramsey ("Ramsey Decl."). This is clear evidence that service of process to this messaging address is a valid method of notification and that John Doe 1 is aware of this action. Nonetheless, there has been no further response from John Doe 1.

14. **John Does 2 - 82** were served on June 5, 2013, at the email addresses used to register the malicious Internet domains which were the "command and control" infrastructure of the Citadel botnet, as set forth in Appendix A and Appendix C to the Complaint. The Complaint and summons were attached to the emails sent on June 5, 2013. Further, a link to www.botnetlegalnotice.com/citadel was also included in the emails sent on June 5, 2013. Plaintiff's counsel have sent out more than 2,900 emails and messages to email and messaging addresses associated with John Doe Defendants 2-82. There has been no response from any of the John Doe Defendants 2-82 to date in this action.

4. Attempted Notice And Service By Mail And Facsimile

15. Investigation was carried out regarding the mailing addresses and facsimile numbers associated with the Citadel botnet domains. This information appears to have been falsified. For example, I 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. I have also verified instances in which the name used to register domains is a fictitious person and/or the address information used to register domains does not exist. The email addresses associated with the domains 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.

5. **Notice And Personal Service To Defendants Pursuant To The Hague Convention**

16. No valid physical addresses of John Doe Defendants 1-82 were identified, thus, to the extent that the Hague Convention on Service of Process is recognized by the relevant countries, service by this means was not possible.

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

Executed this 21st day of October, 2013.

James M. Hsiao