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.	**FILED UNDER SEAL** Civil Action No. _______________ **DECLARATION OF JOHN WILSON IN SUPPORT OF MICROSOFT'S *EX PARTE* APPLICATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER, SEIZURE ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

I, John Wilson, declare as follows:

1. I am the Director of Sales Engineering for Agari Data, Inc. ("Agari"). I make this declaration in support of Microsoft's *Ex Parte* Application For An Emergency Temporary Restraining Order, Seizure Order And Order to Show Cause Re Preliminary Injunction. 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.

2. Agari specializes in helping companies deploy email authentication standards and policies that instruct email receivers to block messages that claim to be from the customer but that fail the authentication protocols. By deploying the Agari solution, companies are able to reduce criminal abuse of their email domains.

3. The Agari solution utilizes data provided by large mailbox providers to help ensure that every legitimate message sent by an Agari customer is authenticated using at least

one of the two available email authentication standards. Agari is also able to monitor messages that claim to be from a customer-owned domain but which are in fact forgeries. Agari's customers are primarily financial institutions, social networking sites, and e-commerce sites. Agari's customers include such institutions as Capital One, J.P. Morgan Chase, and NACHA (National Automated Clearing House Association). In addition to the three aforementioned customers, Agari also monitored email purporting to be from Microsoft, Keybank, US Bank, and Citibank as part of this action.

4. Agari supports the deployment of DMARC (Domain-based Message Authentication, Reporting & Conformance), a technical specification that utilizes two email authentication protocols: Sender Policy Framework ("SPF") and DomainKeys Identified Mail ("DKIM"). SPF seeks to prevent email spam by ensuring the computer sending an email message is on a list of hosts authorized to use the domain for sending email. DKIM seeks to prevent email spam by applying a digital signature to email as it leaves the customer's infrastructure. Both SPF and DKIM provide a mechanism whereby the receiving mailbox provider can determine the authenticity of the email message.

5. I have been Director of Sales Engineering for Agari since 2010. In my role as Director of Sales Engineering, I work with prospective customers to enable global visibility into their use and criminals abuse of the email channel. I teach them best practices with regards to deploying SPF and DKIM. I assist prospective customers as they leverage Agari's reports and alerts to improve the accuracy of their SPF and DKIM deployments. I answer questions about SPF and DKIM and provide demonstrations of Agari's web-based portal.

6. Prior to my current role, I worked as the Chief Technology Officer for Brandmail Solutions, Inc. ("Brandmail"). Brandmail was a solution deployed at mailbox providers that

would check the DKIM signature of incoming messages and either block the message if the signature was missing or invalid or else provide a positive visual indicator in the receiver's webmail interface for messages which passed the DKIM signature validation. In my role as Brandmail CTO, I was required to have an in-depth technical understanding of email authentication in general and the DKIM standard in particular. A true and correct copy of my current *curricula vitae* is attached hereto as Exhibit 1.

7. I began my investigation into botnet activity, and specifically Citadel botnet activity, on December 28, 2012. Agari receives email message data from a number of major email service providers of any email messages that falsely represent themselves to be from one of Agari's customers. These inauthentic emails are detected because they fail both of the security protocols in the authentication schemes supported by Agari.

8. Email messages that have failed both security protocols are likely to be from spammers or other individuals or organizations seeking to convince the receiver that the email is authentic when it is not legitimate. Through my role and experience, the vast majority of the emails that fail both the SPF and DKIM authentication schemes are spam, phishing, and/or exploit-kit infected emails.

9. In an average month, Agari observes approximately 370 million emails that have failed both authentication protocols. I have conducted an assessment on those emails that have failed both authentication protocols. Based upon the assessment, and through my role and experience, approximately 10% of those emails are related to botnet infection attempts, including ones for the Citadel botnet. Furthermore, approximately 35% of those emails contain, display or otherwise use registered trademarks, corporate logos, and other copyrighted assets of Agari's clients.

10. I conclude based on the foregoing that the Citadel botnets have caused, and continue to cause, extreme damage to Agari's clients, including members of the financial industry, consumers and the public at large.

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 27th day of May, 2013

John Wilson