Randall D. Haimovici (*Pro Hac Vice Approved*)
rhaimovici@shb.com
Rachael M. Smith (*Pro Hac Vice Approved*)
rxsmith@shb.com
SHOOK, HARDY & BACON L.L.P.
One Montgomery, Suite 2700
San Francisco, California 94104-4505
Telephone: 415.544.1900
Facsimile: 415.391.0281

Tony M. Diab (Nevada State Bar No. 12954)
tdiab@shb.com
SHOOK, HARDY & BACON L.L.P.
5 Park Plaza, Suite 1600
Irvine, California 92614-2546
Telephone: 949.475.1500
Facsimile: 949.475.0016

Robert J.B. Flummerfelt (Nevada State Bar No. 11122)
rflummerfelt@hotmail.com
Rami Hernandez (Nevada State Bar No. 13146)
rhernandeznsj@hotmail.com
CANON LAW SERVICES, LLC
7251 W. Lake Mead Blvd., Suite 300
Las Vegas, Nevada 89128
Telephone: 702.562.4144
Facsimile: 702.866.9868

Attorneys for Plaintiff
MICROSOFT CORPORATION

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

MICROSOFT CORPORATION, Plaintiff, vs. NASER AL MUTAIRI, an individual; MOHAMED BENABDELLAH, an individual; VITALWERKS INTERNET SOLUTIONS, LLC, d/b/a NO-IP.com; and DOES 1-500, Defendants.	Case No. 2:14-cv-00987-GMN-GWF **SUPPLEMENTAL DECLARATION OF JASON LYONS IN SUPPORT OF APPLICATION OF MICROSOFT COPRORATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE REGARDING A PRELIMINARY INJUNCTION**

I, Jason Lyons, declare as follows:

1. I am a Senior Investigator in the Digital Crimes Unit of Microsoft Corporation's Legal and Corporate Affairs group. I make this supplemental declaration in support of Microsoft's Application for an Emergency Temporary Restraining Order and Order to Show Cause Regarding 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 discussed in this declaration.

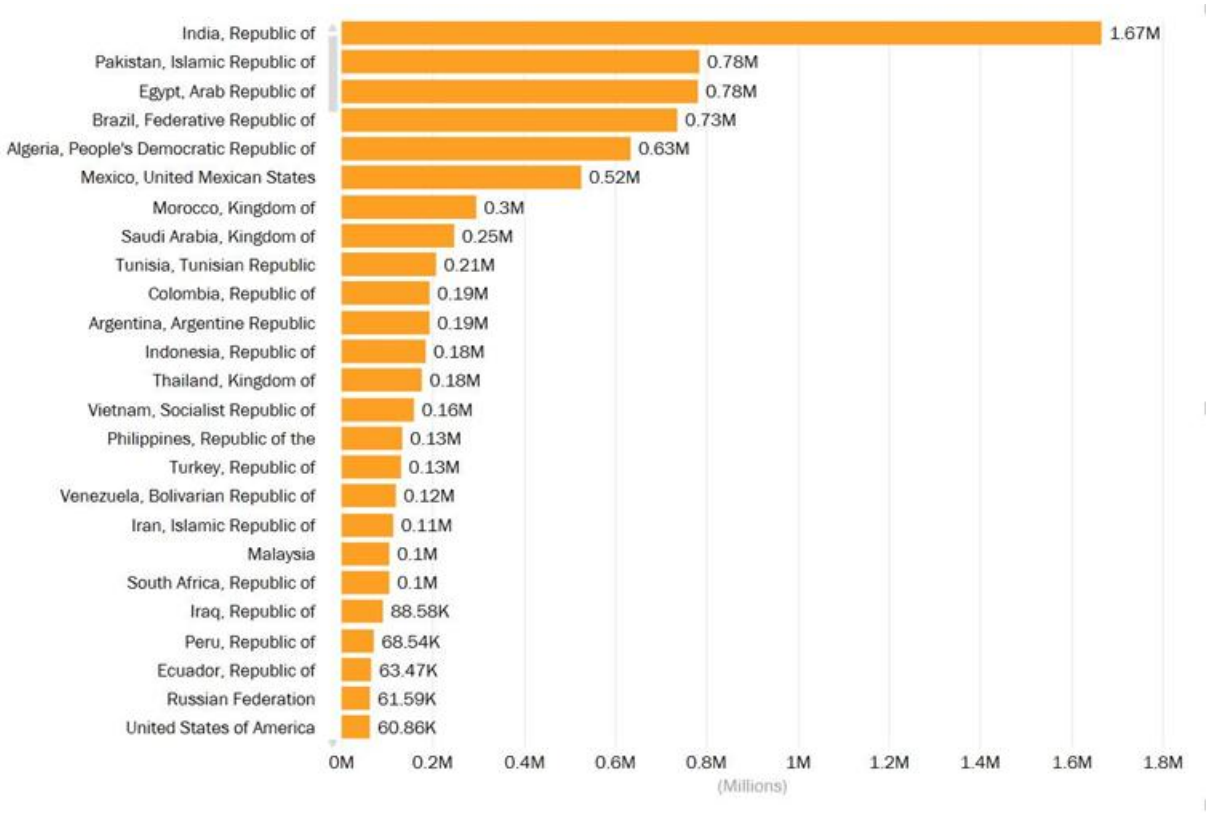
2. This Court issued a Second Amended Temporary Restraining Order ("TRO") ordering that the traffic to the 22 domains owned by Vitalwerks Internet Solutions, LLC ("Vitalwerks"), listed in Appendix B to the TRO, be redirected by the registry operators to Microsoft's servers.

3. On June 30, 2014, the registry operators executed the TRO and redirected the traffic to these domains to Microsoft (the "transfer"). After the transfer, we have been able to monitor the traffic to the sub-domains listed in Appendix A to the TRO that Microsoft has identified as being associated with malware ("Appendix A sub-domains"). As a result, Microsoft has been able to identify the type(s) of malware communicating through the sub-domain, the IP address of the infected computer, and the geographical location of the infected computer.

4. Based on data collected from the date of the transfer on June 30, 2014 through July 5, 2014, we detected over 9.4 million unique IP addresses that are infected with some form of malware, most of which was the Bladabindi and Jenxcus malware. The term "unique IP addresses" only counts every IP address once regardless how many times the IP address reaches out to an Appendix A sub-domain. To say that Microsoft detected 9.4 million infected computers would be a conservative estimate because most IP addresses control about four personal computers and if the IP address is used for a business, it can control more than that. Thus, it is very likely that the number of infected machines detected in that first week is substantially greater than 9.4 million.

5. Moreover, the data indicates that 239 countries have been affected by the malware infections. The following chart indicates the countries with the highest number of unique, infected IP addresses.

Unique Infected IPs by Country

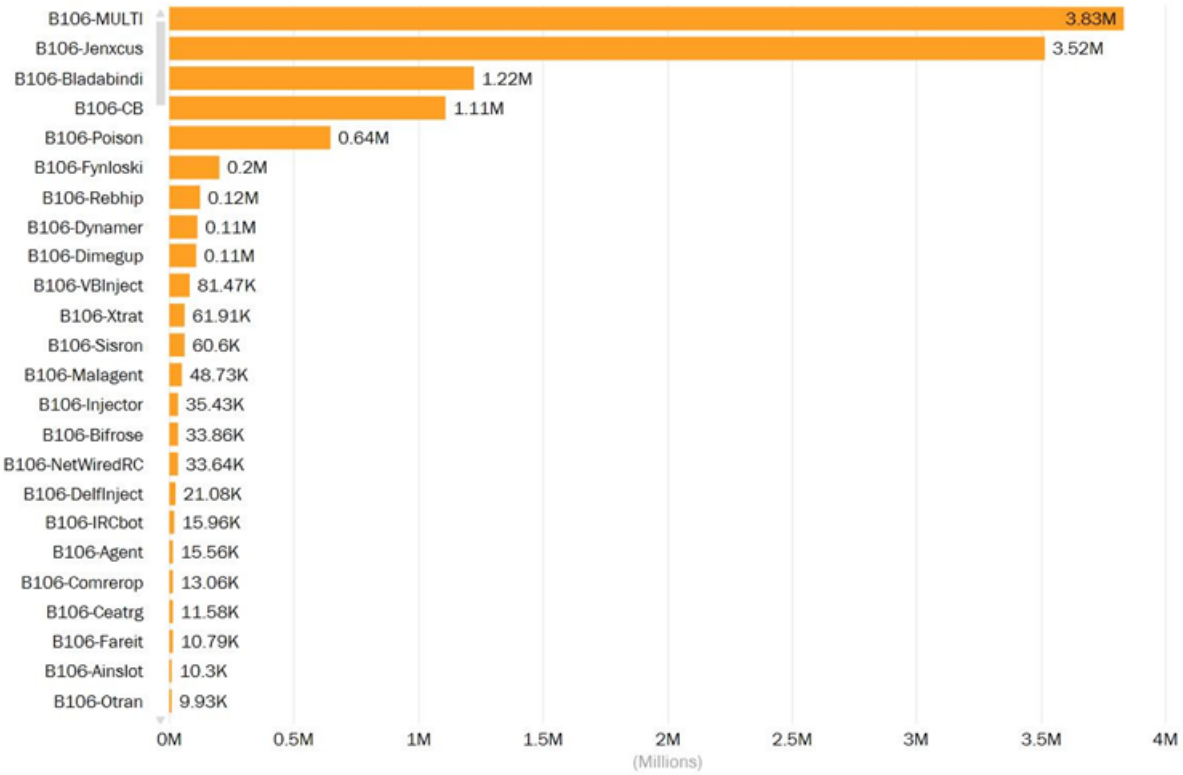


6. Although Microsoft's investigation has been focused on Bladabindi and Jenxcus malware, in the first week of the transfer, Microsoft detected 199 different malware families. The chart below shows the malware families that have the highest number of unique, infected IP addresses. Bladabindi and Jenxcus malware are responsible for 5.85 million unique, infected IP addresses. In fact, 1.11 million of those are infected with both Bladabindi and Jenxcus (indicated on the chart below as "CB").

//

//

Unique Infected IPs by Threat



7. Other malware families, such as Poison and Fynloski, have a significant presence as well. Poison is a family of backdoor Trojans that can give a hacker unauthorized access and control of the infected computer. Fynloski also gives the hacker control over the infected computer, permitting the hacker to execute various functions such as recording your personal information or downloading additional malware.

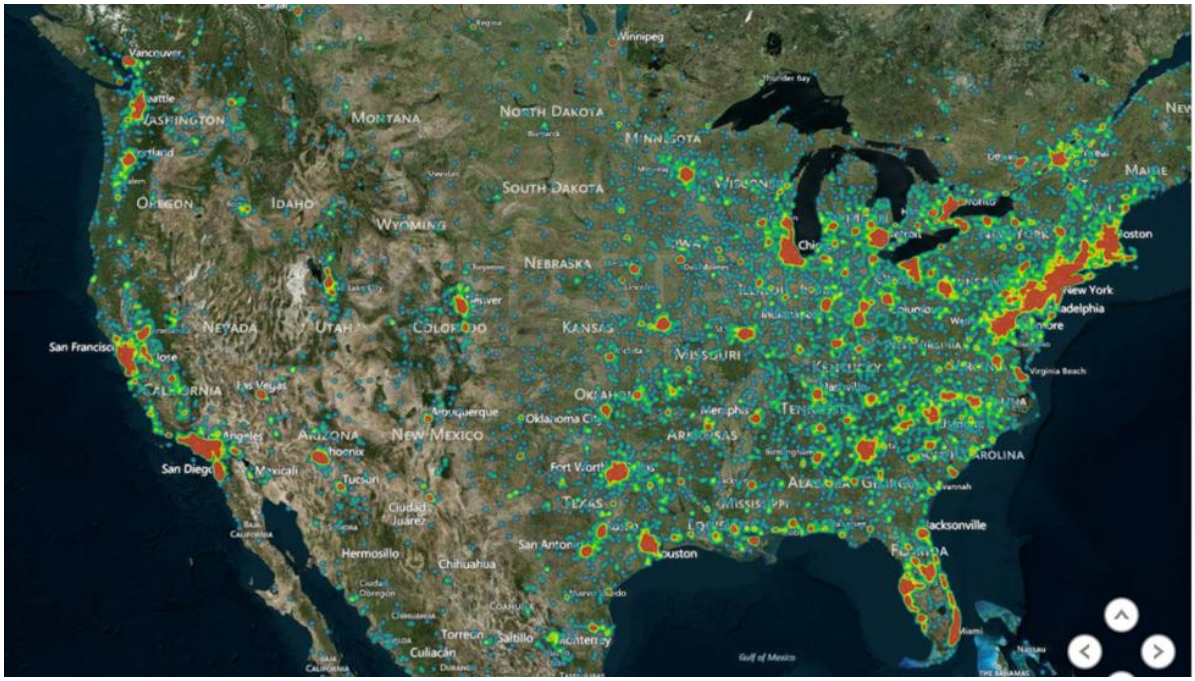
8. Below are heat maps indicating where there are concentrations of unique IP addresses that are infected with the malware (such as Bladabindi and Jenxcus).

//

//

LAS VEGAS, NEVADA

UNITED STATES



WORLD

9. Microsoft is in the process of working with Internet Service Providers and country CERTs to notify victims that they have been infected with one or more of the 199 malware families. Because of the type of malware involved, these victims are more than likely not aware that their computers are infected. Despite Microsoft's efforts to notify victims, the harm caused by the Bladabindi and Jenxcus malware will likely continue unless the individuals responsible for distributing the malware are stopped.

10. Last, I have reviewed the letter that was sent by Roger M. Loeb to the Court, ECF Dkt. No. 32, in which he claims that the transfer disrupted his ability to connect with his server through the use of a Vitalwerks' sub-domain, "martech.noip.us." However, "noip.us" is not one of the second-level domains whose traffic was redirected to Microsoft's servers. So traffic to any sub-domain of "noip.us" would not have been interrupted by the transfer.

//

//

I declare under the 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 on 9th day of July, 2014.

Jason Lyons