The Honorable James L. Robart

UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

AT SEATTLE

MICROSOFT CORPORATION,

Plaintiff,

v.

JOHN DOES 1-11 CONTROLLING A COMPUTER BOTNET THEREBY INJURING MICROSOFT AND ITS CUSTOMERS,

Defendants.

Case No. 2:11-cv-00222

MICROSOFT CORPORATION'S STATUS REPORT RE PRELIMINARY INJUNCTION

INTRODUCTION

On March 9th, 2011, the Court issued the Second Amended *Ex Parte* Temporary Restraining Order, Seizure Order and Order to Show Cause re Preliminary Injunction (the "TRO"). Pursuant to the TRO, Microsoft, in conjunction with the United States Marshals Service effectively disabled a number of IP addresses and domains used by the Rustock botnet to conduct its illegal activity and collected information related to the entities and individuals controlling the content at those IP addresses and domains. This has frustrated, during the pendency of this action, Rustock's ability to send out trademark-infringing spam promoting counterfeit pharmaceuticals and other illegal online activities.

Microsoft Corporation ("Microsoft"), through counsel, now respectfully submits this status

Orrick Herrington & Sutcliffe LLP
701 5th Avenue, Suite 5600
Seattle, Washington 98104-7097
tel+1-206-839-4300

report to assist the Court in its consideration of the relevant issues related to the April 6, 2011 hearing on Microsoft's motion for a preliminary injunction. Set forth below are the results of Microsoft's efforts to provide notice of the preliminary injunction hearing undertaken since March 18, 2011. It is Microsoft's position that Defendants have been provided sufficient notice of the preliminary injunction hearing and that a preliminary injunction should issue during the pendency of this action, as detailed in Microsoft's Application for an Emergency Temporary Restraining Order, Seizure Order and Order to Show Cause re Preliminary Injunction (the "Application") and as set forth below and in the declarations in support of preliminary injunction submitted with this report.

NO CUSTOMERS OF THE IP ADDRESSES OR DOMAINS IN QUESTION HAVE REQUESTD THAT THE IP ADDRESSES OR DOMAINS BE REINSTATED

On March 16, 2011, counsel at Orrick, Herrington & Sutcliffe and the United States Marshals Service personally served copies of all pleadings to the hosting companies listed in Appendix A of the TRO. Ramsey Decl. ¶ 2. Since that point, lawyers from Orrick, Herrington & Sutcliffe LLP have been in continuous contact with the foregoing hosting companies/data centers and also in continuous contact with hosting "resellers" through which the IP addresses were ultimately sold to the defendants. The resellers were located outside the United States. The hosting resellers acted as brokers and sold hosting arrangements at the foregoing U.S. data centers to the defendant end-users. *Id.* ¶ 3. Both the hosting companies and resellers were provided with contact information for Microsoft's outside counsel. *Id.* ¶ 4. The hosting companies and resellers were asked to inform counsel if any of the defendants requested reinstatement of the IP addresses and were asked to have defendants contact counsel about the case if any communication was received from them. *Id.* No hosting company or reseller or domain registrar or registry has requested reinstatement of the IP addresses or domains. *Id.* ¶ 5.

As set forth in greater detail below, Microsoft has continuously gathered contact information for the parties most directly controlling the IP addresses and domains set forth in the TRO and have communicated notice of the preliminary injunction hearing and all pleadings in this action to all such contact information. *Id.* ¶ 6. As of April 4, 2011, Microsoft has received no

Orrick Herrington & Sutcliffe LLP
701 5th Avenue, Suite 5600
Seattle, Washington 98104-7097
tel+1-206-839-4300

request from any of the defendants to reinstate the IP addresses or domains set forth in the TRO and no such request has been conveyed to Microsoft by any hosting company or reseller. *Id.* ¶ 7.

NOTICE AND SERVICE OF PROCESS UPON DEFENDANTS

Microsoft's efforts to give notice of this proceeding to Defendants has been guided by the TRO, which permits notice to be served through any means authorized by law, including 1) personal delivery on Defendants who can be located in the United States; 2) personal delivery through the Hague Convention on Service Abroad on Defendants who can be located outside of the United States; 3) transmission by e-mail, facsimile, and mail to the contact information provided by the Defendants to the data centers providing the IP addresses; and 4) by publishing notice to Defendants on a publicly available Internet website. *See* TRO, 10:15-23. In addition, Microsoft has relied upon wide-spread publicity to provide adequate notice to Defendants of its complaint and this hearing. The following sections summarize Microsoft's efforts to provide adequate notice.

Defendants Are Likely Aware of this Proceeding Given the TRO's Impact

The operation and growth of the Rustock botnet has been frustrated by the temporary restraining order issued by the Court, which was executed on March 16, 2011. *Ramsey Decl*. ¶ 8. Reports indicate that spam output from the Rustock botnet has ceased entirely at that point. *Id.* Information published by security researches and organizations that monitored Rustock, examples of which are attached as Exhibits 1-4 of the Ramsey Declaration, indicate a significant impact on Rustock, with estimates of the reduction in spam volumes worldwide resulting from disabling Rustock as high as 30 to 40 percent. *Id*., Exhibits 1-4. Given the obvious impact on Rustock and the fact that the security research community was aware that the impact was the result of this action, Defendants are likewise also very likely to be aware of the impact on Rustock and to be aware that the instant proceeding is the cause of that impact. *Id*.

Notice and Service by Publication

There is a reasonable likelihood that notice has been effected through publication. On March 18, 2011, Microsoft published the Complaint, copies of each Summons to John Doe Defendants 1-11, all Orders of this Court and all Pleadings in this action on the publicly available

Orrick Herrington & Sutcliffe LLP
701 5th Avenue, Suite 5600
Seattle, Washington 98104-7097
tel+1-206-839-4300

website, www.noticeofpleadings.com. *Id*. ¶ 9, Exhibit 5. While investigation and discovery is ongoing, it appears that Defendants reside in at least Russia and Ukraine, and possibly in other locations as well. *Id*. ¶ 10. The Court's order and the instant action have been widely reported in the media in Russia, Ukraine and elsewhere throughout the world. *See id*., Exhibit 6-8 (exemplary articles from Russian and Ukrainian news outlets along with those of other countries between March 16, 2011 and the present). As discussed below and in the Ramsey Declaration submitted with this report, the link to www.noticeofpleadings.com was provided to all contact information associated with the IP addresses and domains in question.

Notice and Service by Email and Personal Delivery

Pursuant to the Doe discovery provisions in the TRO, the hosting companies associated with the IP addresses set forth in the order provided contact information related to the IP addresses. Thereafter, Microsoft initiated contact with the individuals and entities associated with the IP addresses and provided copies of all pleadings in this action. *Id*. ¶ 11. Most often, the contact information provided by the U.S.-based data centers have been non-U.S. based "resellers" of hosting services at these U.S. datacenters. *Id*. The resellers have provided additional contact information for and contextual information regarding the Defendant end-users who purchased the IP addresses through them. *Id*. Microsoft has initiated contact with the Defendant end-users using the contact information, including email and instant messaging addresses and physical mailing addresses, and provided copies and/or links to all pleadings in this action through those means. *Id*. ¶¶ 11-32. In addition, Microsoft attempted send the same information to the contact information for two other fallback domains: chernomorsky.name and incolonix.com. *Id*. ¶ 33.

Attempted Notice and Service by Facsimile

Notice and service was attempted to the facsimile numbers contained in the records with respect to some of the IP addresses set forth above and also in the WHOIS database for the domains set forth above. None of the facsimile numbers provided by the defendant-customers of the IP addresses or domain registrants are in operation. *Id*. ¶ 34.

Notice and Personal Service to Defendants Pursuant to the Hague Convention

Copies of the Complaint and Orders in this action are being translated into Russian and

Orrick Herrington & Sutcliffe LLP
701 5th Avenue, Suite 5600
Seattle, Washington 98104-7097
tel+1-206-839-4300

Ukrainian, and will be translated into any other relevant languages. *Id.* ¶ 35. To the extent physical addresses can be identified at present and through further Doe discovery, and to the extent that these countries and others recognize the Hague Convention on Service of Process or similar treaties, such documents will be delivered to the appropriate Central Authorities and such authorities will be requested to personally serve the documents on the John Doe defendants at the such physical address information. *Id.* As discussed below, further formal and informal Doe discovery in the United States and in other countries will likely be necessary to discover physical addresses for the Defendants. *Id.* Further, Microsoft is informed and believes that it may take between 3 and 6 months for such Central Authorities to carry out personal service once the process is initiated. Given that the investigation to date reveals errors in the physical addresses and Defendants' efforts to conceal their locations, personal service via the Hague Convention may be challenging, but will be attempted nonetheless. *Id.*

Additional Investigation Regarding Contact Information for Defendants

From the Doe discovery to date, it appears that there are likely a smaller number of actual Defendants managing the botnet command infrastructure than the currently named John Does 1-11. *Id.* ¶ 36. Additional formal and informal discovery is needed in an attempt to identify the Defendants and obtain additional physical contact information for them. *Id.* For example, one source of discovery is companies and domains supporting email addresses used by Defendants set forth above. *Id.* Further, beyond the information set forth in this declaration, Microsoft and its counsel are in possession of additional potential sources of information, including financial accounts and Internet service and email accounts. *Id.* The operators of these accounts are likely to have further information regarding the identities and locations of the Defendants. *Id.* Moreover, through counsel in Moscow, formal and informal discovery processes are being initiated to simultaneously learn additional information regarding the Defendants' identities and locations. *Id.* Promptly after the preliminary injunction proceeding, Microsoft anticipates filing a motion seeking ordinary John Doe discovery, beyond the very specific discovery granted in the TRO itself and will request several months to carry out these efforts. *Id.*

Orrick Herrington & Sutcliffe LLP
701 5th Avenue, Suite 5600
Seattle, Washington 98104-7097
tel+1-206-839-4300

SUPPLEMENTATION OF APPENDIX B

Following the March 16, 2011 implementation of the TRO, Microsoft continued to monitor a number of Rustock-infected end-user computers under its direct observation. Declaration of David Anselmi In Support of Microsoft Corporation's Application for an Emergency Temporary Restraining Order, Seizure Order and Order to Show Cause Re Preliminary Injunction, ¶ 2 (While submitted with this status report, this declaration is in support of the Application.). Through this monitoring, Microsoft determined that some Rustock-infected end-user computers are pre-programmed to attempt to contact the Rustock Command and Control Tier through a previously undetected domain called "incolonix.com." *Id*. In order to keep all or part of the Rustock botnet from contacting Rustock command and control servers through this domain, it is necessary to keep this domain from being owned or operated by the operators of Rustock. *Id*. In addition, Microsoft continued to force the Rustock-infected end-user computers under its direct observation to generate the dynamically-generated domain names through which the Rustock-infected end-user computers will attempt to contact Rustock at future dates. *Id*. In order to keep all or part of the Rustock botnet from contacting Rustock command and control servers through these domains, it is necessary to keep them from being registered by the operators of Rustock. *Id*. Both incolonix.com and the dynamically-generated domains for the May 1-June 30, 2011 time period have been added to Appendix B to the [Proposed] Order for Preliminary Injunction.

Orrick Herrington & Sutcliffe LLP
701 5th Avenue, Suite 5600
Seattle, Washington 98104-7097
tel+1-206-839-4300

Dated: April 4, 2011.

ORRICK, HERRINGTON & SUTCLIFFE LLP

By: s/Jeffrey L. Cox

Jeffrey L. Cox (WSBA No. 37534)
jcox@orrick.com
Ranjit Narayanan (WSBA No. 40952)
rnarayanan@orrick.com

701 5th Avenue
Suite 5600
Seattle, WA 98104-7097
Telephone: +1-206-839-4300
Facsimile: +1-206-839-4301

Of counsel:
Gabriel M. Ramsey (*pro hac vice* application pending)
gramsey@orrick.com
Jacob M. Heath (*pro hac vice* application pending)
jheath@orrick.com

1000 Marsh Road
Menlo Park, CA 94025
Telephone: +1-650-614-7400
Facsimile: +1-650-614-7401

Attorneys for Plaintiff Microsoft Corp.