

Those cybercriminals use the infected computers to conduct illegal activity.

3. As counsel of record for Microsoft, I have participated in Microsoft's previous efforts to disable other computer botnets, including the "**Waledac**" Botnet in February 2010 in the Eastern District of Virginia, the "**Rustock**" Botnet in March 2011 in the Western District of Washington, the "**Kelihos**" Botnet in September 2011 in the Eastern District of Virginia, the "**Zeus**" Botnets in March 2012 in the Eastern District of New York, and the "**Bamital**" Botnet in February 2013 in the Eastern District of Virginia. Based on my previous experience with similar botnet-defendants, *ex parte* relief is necessary, as notice to Defendants would allow them to destroy the evidence of their illicit activity and give them an opportunity to move the instrumentalities they used to conduct their unlawful activity. This would render the further prosecution of this matter futile. Based on my prior experience, I am aware that in one previous effort to disable the Rustock Botnet, the operators of the Rustock Botnet – after learning of the attempt to disable the botnet – managed to migrate that botnet's command and control infrastructure to new IP addresses. The Rustock-infected computers were then directed to new IP addresses.

4. Microsoft's counsel has not attempted to provide notice of the Application to Defendants, and notice should not be required to provide notice at this time. I respectfully submit that good and sufficient reasons exist for this Application to be made by Order to Show Cause in lieu of by notice of motion. Microsoft has previously sought *ex parte* temporary restraining orders in the United States District Court case in *Microsoft Corporation v. John Does 1-27*, Case No. 1:10-cv-00156 (E.D. Va. 2010) (Brinkema, J.); *Microsoft v. John Does, 1-11*, Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.); *Microsoft Corporation v. Dominique Piatti et al.*, Case No. 1:11-cv-01017 (E.D. Va., 2011) (Cacheris, J.); *Microsoft Corporation et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.); *Microsoft Corporation v. Peng Yong et al.*, Case No. 1:12-cv-1005-GBL (E.D. Va. 2012) (Lee, J.); *Microsoft Corp. v. John Does 1-18 et al.*, Case No. 1:13-cv-139-LMB/TCB (E.D. Va. 2013) (Brinkema, J.); *Microsoft v. John Does 1-82*, Case

No. 3:13-CV-00319-GCM (W.D. N.C. 2013) (Mullen, J.). Microsoft, however, has not sought previously this particular *ex parte* relief in this district as to these particular Defendants.

5. Microsoft has identified certain IP addresses (unique numerical for computers throughout the world that connect to the Internet) and Internet domains as part of the command and control infrastructure of the ZeroAccess botnet. The IP addresses and Internet domains associated with ZeroAccess' command and control infrastructure and the contact information for registrants of the IP addresses and Internet domains are set forth at Appendix A to the Complaint. A true and correct copy of Appendix A to the Complaint is attached hereto as **Exhibit 1**.

6. I have conducted research in an effort to identify Defendants associated with these IP addresses and Internet domains. I have been unable to determine the true identities of Defendants. I have confirmed that registration information is decisively false. Based on my prior experience and based on my research regarding these IP addresses and Internet domains, it is likely that further contact information has been provided by Defendants to the hosting companies and Internet domain name registrars through the IP address and Internet domain registration process. This information may include individual and entity names, physical addresses, email addresses, facsimile numbers, and telephone numbers. I have reviewed the requirements to sign up for services and the terms of service relating to the Internet domains and IP addresses and conclude, based on this research, that such contact information is likely to be in the possession of the hosting companies and Internet domain registrars.

7. To the extent Defendants have provided such information, the information most likely to be accurate are e-mail addresses as, upon information and belief, such are necessary to register IP addresses or Internet domains. It is more likely that the email addresses exist and are functional than it is likely that the personal names and physical addresses are correct or accurate. I conclude this in part based on the fact that when

registrants set up IP addresses and Internet domains they must receive confirmation from the hosting company and Internet domain registrars via email in order to utilize and access the IP addresses and Internet domains. Other contact information, such as physical address information, is more likely to be false. I base this conclusion, in part, on past experiences relating to botnets in which IP address or domain registration name, address and telephone number were determined to be fraudulent or stolen, but the email address provided by defendants was, in fact, associated with them. Further supporting this conclusion, in May 2010, the Internet Corporation for Assigned Names and Numbers (“ICANN”) – an organization that administers the domain name system – issued a study indicating the ease with which name and physical mailing addresses for domain registrations may be falsified. Attached hereto as **Exhibit 2** is a true and correct copy of the ICANN’s May 2010 study, “WHOIS Proxy/Privacy Service Abuse – Definition.”

8. Based on my prior experience and from my research, I believe that the most reliable contact information for effecting communication with Defendants are email addresses that have been discovered to be associated with Defendants IP addresses or domains, and the contact information, particularly email addresses, in possession of the hosting company and Internet domain registrars. From my research, I conclude that such contact information is likely to be valid, as it is necessary to obtain web hosting services or Internet domain names. Upon provision of such contact information by the web hosting companies and Internet domain registries to Microsoft, notice of this proceeding and service of process may be attempted using such contact information. Through my research, I have not discovered any other information that would enable, at this point, further identification of or contact with Defendants other than that in the possession of these companies. I believe that absent an order directing Doe discovery, these companies will be unlikely to share contact information necessary to provide notice and service to Defendants.

II. NOTICE AND SERVICE OF PROCESS

A. Microsoft Has Robust Plans To Provide Notice

9. On behalf of Microsoft, Orrick will attempt notice of any TRO and preliminary injunction hearing, as well as service of the Complaint by sending the pleadings and/or links to the pleadings to e-mail addresses, facsimile numbers and mailing addresses associated with Defendants or otherwise provided by Defendants to the IP address hosting companies and Internet domain registrars.

10. On behalf of Microsoft, Orrick will attempt notice of any TRO, preliminary injunction hearing and service of the complaint by publishing those pleadings on a publicly accessible website located at: www.botnetlegalnotice.com/ZeroAccess. Orrick will publish such notice, in English, in Russian and in any other language determined to be relevant, on the website for a period of six months. The following information will be made available on the website:

- a. The information contained in the case caption and the content of the summons.
- b. The following summary statement of the object of the complaint and the demand for relief: "Plaintiff Microsoft Corporation ("Microsoft") has sued defendants John Does 1-8 associated with the IP addresses and Internet domains listed in the documents submitted in this action. Microsoft alleges that Defendants have violated Federal and state law by operating a computer botnet through these IP addresses and domains, causing unlawful intrusion into Microsoft's and its customers' computers, intellectual property violations, and click-fraud to the injury of Microsoft, its customers, and the public. Microsoft seeks a preliminary injunction order directing the Internet Service Providers to take all steps necessary to disable communications between the IP addresses listed in the documents submitted in this action and computers on the ISPs' respective networks

and to ensure that changes or access to the IP addresses so that Defendants or Defendants' representatives or any other person, is unable to access those IP addresses, except as provided by the Court's order. Microsoft also seeks a preliminary injunction order directing the registry associated with these Internet domains to redirect them to secure servers and ensure that Defendants cannot change or access the domains. Microsoft seeks a permanent injunction, other equitable relief and damages. Full copies of the pleading documents are available at www.botnetlegalnotice.com/ZeroAccess."

- c. The date of first publication.
- d. The following text: "NOTICE TO DEFENDANT: READ THESE PAPERS CAREFULLY! You must "appear" in this case or the other side will win automatically. To "appear" you must file with the court a legal document called a "motion" or "answer." The "motion" or "answer" must be given to the court clerk or administrator within 21 days of the date of first publication specified herein. It must be in proper form and have proof of service on the Microsoft's attorneys, David Hoffman at Fish & Richardson, One Congress Plaza, Suite 810, 111 Congress Avenue, Austin, Texas, 78701 or Gabriel M. Ramsey at Orrick, Herrington & Sutcliffe LLP, 1000 Marsh Rd., Menlo Park, California, 94025. If you have questions, you should consult with your own attorney immediately."

11. On behalf of Microsoft, Orrick will serve each of hosting companies and the Internet domain registries listed at Appendix A to the Complaint and the Internet Service Providers listed at Appendix B to the Complaint with copies of all documents served on Defendants.

12. On behalf of Microsoft, Orrick will retain a national service of process firm to attempt notice of any TRO and preliminary injunction hearing, as well as service of the

complaint by personal delivery on any Defendant in this case that has provided accurate contact information in the United States. Upon execution of any TRO, Orrick will instruct the process server to deliver these documents to any accurate U.S. addresses associated with Defendants.

13. On behalf of Microsoft, Orrick will prepare Requests for Service Abroad of Judicial or Extrajudicial Documents to attempt notice of any TRO and preliminary injunction hearing, as well as service of the Complaint on any Defendants in this case that have provided accurate contact information in foreign countries that are signatories to the Hague Convention on Service Abroad or any similar treaty, and will comply with the requirements of those treaties. Upon entry of any TRO, Orrick will execute and deliver these documents to the appropriate Central Authority and request, pursuant to the Hague Convention or similar treaty, that the Central Authority deliver these documents to the contact information provided by Defendants. I am informed, and therefore believe, that notice of the preliminary injunction hearing and service of the Complaint could take approximately three to six months or longer through this process.

B. Notice Under ICANN Domain Name Registration Policies

14. Attached hereto as **Exhibit 3** is a true and correct copy of a document describing ICANN's role. Exhibit 3 reflects the following. ICANN is a not-for-profit partnership formed in 1998. ICANN coordinates domain names and IP addresses (unique identifying numbers for computers throughout the world), which enables the operation of the global Internet. ICANN's responsibilities include running an accreditation system for domain name "registrars." Internet domain name registrars enter into arrangements with individual "registrants" who wish to register particular domain names. ICANN has a contractual relationship with all accredited registrars that set forth the registrars' obligations. The purpose of the requirements of ICANN's accreditation agreements with registrars is to provide a consistent and stable environment for the domain name system, and hence the Internet.

15. A true and correct copy of the accreditation agreement between ICANN and domain name registrars in use before May 21, 2009 is attached hereto as **Exhibit 4**.

16. A true and correct copy of the accreditation agreement between ICANN and domain name registrars in use on or after May 21, 2009 is attached hereto as **Exhibit 5**.

17. The following summarizes provisions set forth in the ICANN accreditation agreements with registrars at Exhibits 4 and 5.

1. **ICANN Requires That Registrants Agree To Provide Accurate Contact Information**

18. Section 3.7.7.1 of the accreditation agreement provides that domain registrants will provide the registrar accurate and reliable contact information. In particular, the domain name registrant:

“shall provide to Registrar accurate and reliable contact details and promptly correct and update them during the term of the Registered Name registration, including: the full name, postal address, e-mail address, voice telephone number, and fax number if available of the Registered Name Holder; name of authorized person for contact purposes in the case of an Registered Name Holder that is an organization, association or corporation....”

19. Section 3.7.7.2 of the accreditation agreement provides that if the registrant fails to respond for over 15 days to a registrar’s inquiry about inaccurate contact information, the domain may be cancelled. In particular, the domain name registrant’s:

“willful provision of inaccurate or unreliable information, its willful failure to promptly update information provided to Registrar, or its failure to respond for over fifteen (15) calendar days to inquiries by Registrar concerning the accuracy of contact details associated with the Registered Name Holder’s registration shall constitute a material breach of the Registered Name Holder-registrar contract and be a basis for cancellation of the Registered Name registration.”

2. **ICANN Requires That Registrants Agree To A Dispute Resolution Policy Under Which Notice Is Given By Sending The Complaint To The Registrant’s Contact Information**

20. Section 3.8 of the accreditation agreement provides that registrars shall require registrants to agree to the Uniform Domain Name Dispute Resolution Policy (“UDRP”). The UDRP is a policy between a registrar and its customer and is included in registration agreements

for all ICANN-accredited registrars. Attached hereto as Exhibit 6 is a true and correct copy of the UDRP.

21. As part of the registrant's agreement to the UDRP, the registrant agrees to the Rules for Uniform Domain Name Dispute Resolution Policy ("Rules"). Attached hereto as Exhibit 7 is a true and correct copy of the Rules.

22. Pursuant to the Rules, "Written Notice" of a complaint regarding a domain requires electronic transmittal of the complaint to a domain registrant and hardcopy notification that the complaint was sent by electronic means. In particular, "Written Notice" is defined as:

"hardcopy notification by the Provider to the Respondent of the commencement of an administrative proceeding under the Policy which shall inform the respondent that a complaint has been filed against it, and which shall state that the Provider has electronically transmitted the complaint including any annexes to the Respondent by the means specified herein. Written notice does not include a hardcopy of the complaint itself or any annexes."

23. Pursuant to the Rules, notice of a complaint may be achieved by the registrar forwarding the complaint to the postal address, facsimile number and e-mail addresses of the domain registrant. In particular, the Rules define the procedure for providing notice as follows:

"(a) When forwarding a complaint, including any annexes, electronically to the Respondent, it shall be the Provider's responsibility to employ reasonably available means calculated to achieve actual notice to Respondent. Achieving actual notice, or employing the following measures to do so, shall discharge this responsibility:

(i) sending Written Notice of the complaint to all postal-mail and facsimile addresses (A) shown in the domain name's registration data in Registrar's Whois database for the registered domain-name holder, the technical contact, and the administrative contact and (B) supplied by Registrar to the Provider for the registration's billing contact; and

(ii) sending the complaint, including any annexes, in electronic form by e-mail to:

(A) the e-mail addresses for those technical, administrative and billing contacts;

(B) postmaster@<the contested domain name>; and

(C) if the domain name (or "www." followed by the

domain name) resolves to an active web page other than a generic page the Provider concludes is maintained by a registrar or ISP for parking domain-names registered by multiple domain-name holders), any e-mail address shown or e-mail links on that web page; and

(iii) sending the complaint, including any annexes, to any e-mail address the Respondent has notified the Provider it prefers and, to the extent practicable, to all other e-mail addresses provided to the Provider by Complainant...”

24. The effect of the UDRP and the Rules is that domain name registrants agree that notice of a complaint relating to their domains may be provided by the foregoing means, including by sending the complaint to postal, facsimile and email addresses provided by registrants.

3. **ICANN Requires That Registrants Agree That Domains May Be Suspended Or Cancelled Pursuant To The Dispute Resolution Policy**

25. Section 3.7.7.11 of the accreditation agreement provides that registrars shall require that a domain name registrant “shall agree that its registration of the Registered Name shall be subject to suspension, cancellation or transfer” pursuant to ICANN’s policies for the resolution of disputes concerning domain names.

4. **ICANN Requires That Registrants Agree Not To Use Domains In An Illegal Manner**

26. Under Section 2 of the UDRP, the domain registrant agrees that:

“By applying to register a domain name, or by asking us to maintain or renew a domain name registration, you hereby represent and warrant to us that (a) the statements that you made in your Registration Agreement are complete and accurate; (b) to your knowledge, the registration of the domain name will not infringe upon or otherwise violate the rights of any third party; (c) you are not registering the domain for an unlawful purpose; and (d) you will not knowingly use the domain name in violation of any applicable laws or regulations. It is your responsibility to determine whether your domain name registration infringes or violates someone else’s rights.”

27. Similarly, section 3.7.7.9 of the accreditation agreement provides that the domain name registrant “shall represent that, to the best of the Registered Name Holder’s knowledge and belief, neither the registration of the Registered Name nor the manner in

which it is directly or indirectly used infringes the legal rights of any third party.”

C. **Notice Under Web Hosting Companies Terms, Conditions, Policies, And Service Agreements**

1. **Hosting Companies And Internet Domain Registrars Send Account-Related Information To Customer-Provided Contact**

28. The terms of service of the hosting companies and the Internet domain registrars provide for sending account-related notices to contact information provided by the customers, including, on information and belief, Defendants. For example, the terms and conditions for hosting companies **Root S.A.** (“Root”), **Private Layer Inc.** (“Private Layer”), and **RN Data SIA** (“RN Data”) – through which Defendants registered IP addresses – provide that their customers must provide contact information, including the email address, postal address, and a valid home phone number where they can reach their customers. These hosting companies further provide that they may contact their respective customers based on the information their customers provided. A true and correct copy of Root’s “General Terms and Conditions” and “Specific Terms and Conditions” is attached hereto as **Exhibit 8**. A true and correct copy of Private Layer’s “Enhanced Privacy Policy” is attached hereto as **Exhibit 9**. A true and correct copy of RN Data’s “Acceptable Use Policy” is attached hereto as **Exhibit 10**.

29. The terms of service for Internet domain registrars’ **eNom, Inc.** (“eNom”), **NameCheap, Inc.** (“NameCheap, Inc.”), and **GoDaddy.com LLC** (“GoDaddy”) provides that their customers must provide contact information, including the email address, postal address, and a valid home phone number where they can reach their customers. These Internet domain registrars further provide that they may contact their respective customers based on the information provided by that customer. A true and correct copy of eNom’s “Privacy Policy” is attached hereto as **Exhibit 11**. A true and correct copy of eNom’s “Registration Agreement” is attached hereto as **Exhibit 12**. A true and correct copy of NameCheap’s “Privacy Policy” is attached hereto as **Exhibit 13**. A true and correct copy of NameCheap’s “Registration Agreement” is attached hereto as **Exhibit 14**. A true and

correct copy of GoDaddy's "Domain Name Registration Agreement" is attached hereto as **Exhibit 15**. A true and correct copy of GoDaddy's "Privacy Policy" is attached hereto as **Exhibit 16**.

30. Based on my past experience and my research of third parties that Defendants use to provide domain name and web hosting services, the other third party Internet hosting companies and Internet domain name registrars require that similar contact information be provided.

2. **Web Hosting And Internet Domain Name Registrars Terms Of Service Prohibit Customers From Using Services In An Illegal Manner**

31. The Internet domain registrars and web hosting terms of service prohibit customers, including, on information and belief, Defendants, from use the services in an illegal manner, and customer accounts may be terminated for violation of those terms. Root's, Private Layer's, RN Data's, eNoms's, GoDaddy's, and NameCheap's policies all prohibit, among other conduct:

- a. tampering with system resources or accounts of other customers or of any other Internet sets, networks, or private or public domains;
- b. transmitting or distributing copyrighted, trademarked, trade secret, or other Intellectual property without proper authorization;
- c. manufacturing, using, or distributing counterfeit, pirated, or illegal software;
- d. storing, distributing, or transmitting unlawful material, including computer virus;
- e. spamming, hacking, or engaging in DDoS attacks;
- f. transmitting or distributing child pornographic material; and
- g. facilitating, aiding, or encouraging any of the above activities.

32. Their policies also provide that they may suspend or terminate its customer's services if that customer has been found to engage in prohibited conduct. Based on my past experience and my current research of other Internet domain registrars and hosting companies, and on information and belief, the other Internet domain registrars and hosting companies used by Defendants prohibit similar unlawful conduct.

III. OTHER AUTHORITY AND EVIDENCE

33. Attached hereto as **Exhibit 17** is a true and correct copy of the June 2, 2009 *Ex Parte* Temporary Restraining Order and Order to Show Cause in the matter *FTC v. Pricewert LLC et al.*, Case No. 09-2407 (N.D. Cal., Whyte J.).

34. Attached hereto as **Exhibit 18** is a true and correct copy of the June 15, 2009 *Preliminary Injunction in the matter FTC v. Pricewert LLC et al.*, Case No. 09-2407 (N.D. Cal., Whyte J.).

35. Attached hereto as **Exhibit 19** is a true and correct copy of the Indictment and supporting materials in the criminal case *U.S. v. Ancheta*, Case No. 05-1060 (C.D. Cal. 2005).

36. Attached hereto as **Exhibit 20** is a true and correct copy of the Sentencing in the criminal case *U.S. v. Ancheta*, Case No. 05-1060 (C.D. Cal. May 8, 2006).

37. Attached hereto as **Exhibit 21** is a true and correct copy of the *Ex Parte* Temporary Restraining Order and Order to Show Cause in the matter *Microsoft Corporation v. John Does 1-27*, Case No. 1:10-cv-00156 (E.D. Va., 2010) (Brinkema J.).

38. Attached hereto as **Exhibit 22** is a true and correct copy of the Preliminary Injunction in the matter *Microsoft Corporation v. John Does 1-27*, Case No. 1:10-cv-00156 (E.D. Va., 2010) (Brinkema J.).

39. Attached hereto as **Exhibit 23** is a true and correct copy of the *Ex Parte* Temporary Restraining Order and Order to Show Cause in the matter of *Microsoft v. John Does 1-11*, Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.).

40. Attached hereto as **Exhibit 24** is a true and correct copy of the Preliminary Injunction in the matter *Microsoft Corporation v. John Doe 1-11*, Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.).

41. Attached hereto as **Exhibit 25** is a true and correct copy of the *Ex Parte* Temporary Restraining Order and Order to Show Cause in the matter *Microsoft Corporation v. Dominique Alexander Piatti et al.*, Case No. 1:11-cv-01017 (E.D. Va. 2011) (Cacheris, J.).

42. Attached hereto as **Exhibit 26** is a true and correct copy of the Consent Preliminary Injunction in the matter *Microsoft Corporation v. Dominique Alexander Piatti et al.*, Case No. 1:11-cv-01017 (E.D. Va. 2011) (Cacheris, J.).

43. Attached hereto as **Exhibit 27** is a true and correct copy of the *Ex Parte* Temporary Restraining Order, Seizure Order and Order To Show Cause in the matter of *Microsoft Corporation et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.).

44. Attached hereto as **Exhibit 28** is a true and correct copy of the Consent Preliminary Injunction in the matter of *Microsoft Corporation et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.).

45. Attached hereto as **Exhibit 29** is a true and correct copy of the *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Microsoft Corporation v. Peng Yong et al.*, Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.).

46. Attached hereto as **Exhibit 30** is a true and correct copy of the *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Microsoft Corporation v. John Does 1-18, et al.*, Case No. 1:13-cv-139-LMB/TCB (E.D. Va. 2013) (Brinkema, J.).

47. Attached hereto as **Exhibit 31** is a true and correct copy of the Preliminary Injunction in the matter of *Microsoft Corporation v. John Does 1-18, et al.*, Case No. 1:13-cv-139-LMB/TCB (E.D. Va. 2013) (Brinkema, J.).

48. Attached hereto as **Exhibit 32** is a true and correct copy of the *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter *Microsoft v. John Does 1-82*, Case No. 3:13-CV-00319-GCM (W.D. N.C. 2013) (Mullen, J.).

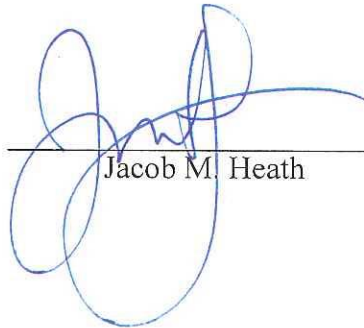
49. Attached hereto as **Exhibit 33** is a true and correct copy of the Preliminary Injunction in the matter of *Microsoft v. John Does 1-82*, Case No. 3:13-CV-00319-GCM (W.D. N.C. 2013) (Mullen, J.).

50. Attached hereto as **Exhibit 34** is a true and correct copy of a March 5, 2012 report entitled "White House Advisor Schmidt Discusses Online Trusted ID Plan, Fighting Botnets."

51. Attached hereto as **Exhibit 35** is a true and correct copy of ICANN's "Guidance for Preparing Domain Name Orders, Seizures & Takedowns."

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

Executed this 24 day of November, 2013 in Austin, Texas.



Jacob M. Heath