IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

MICROSOFT CORPORATION, a Washington corporation, Plaintiff, v. JOHN DOES 1-2, CONTROLLING A COMPUTER NETWORK AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS Defendants.	Civil Action No: **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5**

DECLARATION OF GARYLENE JAVIER IN SUPPORT OF MICROSOFT'S APPLICATION FOR AN *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Garylene Javier, hereby declare and state as follows:

1. I am an attorney with the law firm of Crowell & Moring LLP ("Crowell"), and counsel of record for Plaintiff Microsoft Corporation ("Microsoft"). I make this declaration in support of Microsoft's Application for an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Application"). 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. PARTIES

1. Microsoft seeks an Emergency *Ex Parte* Temporary Restraining Order And Order To Show Cause Re Preliminary Injunction designed to disrupt the technical malicious infrastructure of a sophisticated online criminal network used by Defendants John Does 1-2 ("Defendants") to engage in a spearphishing operation referred to as "Bohrium." Through

Bohrium, Defendants are engaged in using fictitious social media profiles to obtain personal information of the victims. This in turn is used to steal credentials and break into the Microsoft accounts and computer networks of Microsoft's customers and steal highly sensitive information. To manage and direct Bohrium, Defendants have established and operate a network of websites, domains, and computers on the Internet, which they use to target their victims, compromise their online accounts, infect their computing devices, compromise the security of their networks, and steal sensitive information from them.

2. As counsel of record for Microsoft, I am aware of previous efforts to disable other types of unlawful Internet activity, 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, the "**Bamital**" Botnet in February 2013 in the Eastern District of Virginia, the "**Citadel**" Botnets in May 2013 in the Western District of North Carolina, the "**ZeroAccess**" Botnet in November 2013 in the Western District of Texas, the "**Shylock**" Botnet in June 2014 in the Eastern District of Virginia, the "**Ramnit**" Botnet in February 2015 in the Eastern District of Virginia, the "**Dorkbot**" Botnet in November 2015 in the Eastern District of New York; the "**Strontium**" threat infrastructure in August 2016 in the Eastern District of Virginia; the "**Phosphorous**" threat infrastructure in March 2019 in the District of Columbia; the "**Thallium"** threat infrastructure in December 2019 in the Eastern District of Virginia; and "**Trickbot**" threat infrastructure in October 2020 in the Eastern District of Virginia.

3. Based on my previous experience with similar cybercriminal defendants that conduct their operations using an infrastructure consisting of a set of websites, domains and

IP addresses, *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.

4. Based on my experience, for example, I am aware that in an earlier matter attempting to disable the Rustock Botnet, the operators of the Rustock Botnet—after learning of the attempt to disable the botnet—attempted to migrate that botnet's command and control infrastructure to new IP addresses and attempted to delete files from the seized host servers. Similarly, in a prior matter involving the Dorkbot Botnet, its operators attempted to activate previously dormant command and control domains so that they could continue to illegally control the Dorkbot infected devices ***one*** day after Microsoft executed the court's temporary restraining order. Further, during a prior action regarding the ZeroAccess botnet in November 2013, the operators of that botnet immediately attempted (unsuccessfully) to take action, in response to the seizure of domains to attempt to move the botnet's command and control infrastructure. Based on my knowledge of prior similar experiences, I conclude that there is a similar risk that Defendants here would take similar action.

5. Microsoft's counsel has not attempted to provide notice of the TRO Application to Defendants, and should not be required to provide notice at this time. I respectfully submit that good and sufficient reasons exist for this TRO 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 United States District Courts 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 v. John Does 1-8*, Case No. A-13-CV-1014-SS (Sparks, J.) (W.D. Tex 2013); *Microsoft v. John Does 1-8,* Case No. 1:14-cv-811-LO-IDD (O'Grady, J.) (E.D. Va. 2014); *Microsoft v. John Does 1-3,* Case No. 1:15-cv-240-LMB/IDO (Brinkema, J.) (E.D. Va. 2015); *Microsoft v. John Does 1-5,* 1:15-cv-06565-JBW-LB (E.D.N.Y. 2015); *Microsoft Corporation v. John Does 1-2,* Case No. 1:16-cv-993 (E.D. Va. 2016) (Lee, J.); *Microsoft Corporation v. John Does 1-2*, Case No. 1:19-cv-00716-ABJ (D.C. 2019) (Berman-Jackson, J.); *Microsoft Corporation v. John Does 1-2,* Case No. 1:19-cv-01582 (E.D. Va. 2019) (O'Grady, J.); *Microsoft Corporation and FS-ISAC, Inc. v. John Does 1-2,* Case No. 1:20-cv-1171 (E.D. Va. 2020) (Trenga, J.). Microsoft, however, has not previously sought this particular *ex parte* relief in this district as to these particular Defendants.

6. Microsoft has identified certain Internet domains as part of the infrastructure of Defendants. The domains associated with Defendants' infrastructure and the contact information for registrants of the 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**.

7. I understand that members of Microsoft's Digital Crimes Unit, including Christopher Coy, Principal Investigator, have worked to determine the true identities of Defendants. The only publicly available information associated with Defendants' domains

are email addresses. Based on my prior experience and based on Digital Crimes Unit's research regarding these Defendants' domains, it is likely that further contact information has been provided by Defendants to the hosting companies and Internet domain name registrars during the domain name registration and maintenance process. This information may include individual and entity names, physical addresses, email addresses, facsimile numbers, and telephone numbers.

8. To the extent Defendants have provided such information, the information most likely to be accurate are email addresses as, upon information and belief, such are necessary to register Internet domains and associated infrastructure. 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 Internet domains and associated infrastructure they must receive confirmation from the Internet domain registrars or hosting companies via email in order to utilize and access the 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."

9. Based on my prior experience and from Microsoft's 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 domains, and the contact information, particularly email addresses, in possession of the Internet domain registrars or hosting companies. From my research, I conclude that such contact information is likely to be valid, as it is necessary to obtain Internet domain names or web hosting service. Upon provision of such contact information by the Internet domain registrars and web hosting companies 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

10. On behalf of Microsoft, Crowell 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 Internet domain registrars and hosting companies.

11. On behalf of Microsoft, Crowell 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: noticeofpleadings.com/bohrium. Crowell will publish such

notice 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 1-2 associated with the Internet domains listed in the pleading set forth below. Microsoft alleges that Defendants have violated Federal and state law by hosting a cybercriminal operation through these Internet domains, causing or attempting unlawful intrusion into Microsoft and Microsoft's customers' computers, computing devices and/or accounts; and intellectual property violations to the injury of Microsoft and Microsoft's customers. Microsoft seeks a preliminary injunction directing the registries associated with these Internet domains to take all steps necessary to disable access to and operation of this infrastructure to ensure that changes or access to the infrastructure cannot be made absent a court order and that all content and material associated with this infrastructure are to be isolated and preserved pending resolution of the dispute. Microsoft seeks a permanent injunction, other equitable relief and damages. Full copies of the pleading documents are available at noticeofpleadings.com/bohrium."

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, Gabriel M. Ramsey at Crowell & Moring, 3 Embarcadero Center, 26th Floor, San Francisco, CA 94111. If you have questions, you should consult with your own attorney immediately."

12. On behalf of Microsoft, Crowell will serve each of the Internet domain registries listed at **Appendix A** to the Complaint with all copies of all documents served on Defendants.

13. On behalf of Microsoft, Crowell will also 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 existing physical addresses in the United States.

14. On behalf of Microsoft, Crowell 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 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, Crowell 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

15. 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." 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.

16. A true and correct copy of the 2013 ICANN Registrar Accreditation Agreement between ICANN and domain name registrars is attached hereto as **Exhibit 4**.

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

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 correct and update them within seven (7) days of any change 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 update information provided to Registrar within seven (7) days of any change, or its failure to respond for over fifteen (15) 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 suspension and/or cancellation of the Registered Name registration."

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 5** 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 6** 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.

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.

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."

Defendants' Internet Domain Registrars Send Account-Related Information To Customer-Provided Contacts

28. The terms of service for Internet domain registrars used by Defendants provide that their customers must provide contact information, including the email address, postal address, and a valid telephone 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. In particular, NameSilo, LLC's ("NameSilo") General Terms and Conditions, available at https://www.namesilo.com/Support/General-Terms-and-Conditions, include such provisions. Similarly, Key-Systems GmbH's ("Key-Systems") Registration Agreement, available at https://www.key-systems.net/en/registration-agreement, also includes such provisions. A true and correct copy of each NameSilo's General Terms and Conditions and Key-Systems' Registration Agreement are attached hereto as **Exhibit 7**.

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

The Defendants' Internet Domain Name Registrars' Terms Of Service Prohibit Customers From Using Services In An Illegal Manner

30. The Internet domain registrars' terms of service prohibit customers, including Defendants, from using the services in an illegal manner, and customer accounts may be terminated for violation of those terms. For example, NameSilo's agreement prohibits, among other conduct, the registered domain being used to:

a. registration of prohibited domain name(s),

b. abuse of NameSilo's services,

c. payment irregularities,

d. illegal conduct,

e. failure to keep account or WHOIS information accurate and up to date,

f. failure to respond to inquiries from NameSilo for over three (3) calendar days,

g. if use of NameSilo's services involves NameSilo in a violation of any third party's rights or acceptable use policies, including but not limited to the transmission of unsolicited email, the violation of any copyright, or the distribution of any form of malware (defined to include, without limitation, malicious code or software that might affect the operation of the Internet),

h. to comply with any applicable court orders, laws, government rules or requirements, requests of law enforcement or other governmental agency or organization, or any dispute resolution process,

i. to avoid any liability, civil or criminal, on the part of NameSilo, as, well as its affiliates, subsidiaries, officers, directors, and employees,

j. to protect the integrity, security and stability of the Domain Name system (DNS), or

k. failure to respond to inquiries from NameSilo regarding payment inquiries for over 24 hours

31. NameSilo's policies also provide that it 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 on information and belief, the other Internet domain registrars used by Defendants prohibit similar unlawful conduct.

III. OTHER AUTHORITY AND EVIDENCE

32. Attached hereto as **Exhibit 8** is a true and correct copy of the March 15, 2019 *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Microsoft v. John Does 1-2*, Case No. 1:19-cv-00716-ABJ (D.C. 2019) (Berman-Jackson, J.).

33. Attached hereto as **Exhibit 9** is a true and correct copy of the December 18, 2019 *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Microsoft v. John Does 1-2,* Case No. 1:19-cv-01582 (E.D. Va. 2019) (O'Grady, J.).

34. Attached hereto as **Exhibit 10** is a true and correct copy of the May 1, 2020 *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Sophos v. John Does 1*-2, Case No. 1:20-cv-00502 (E.D. Va. 2020) (O'Grady, J.).

35. Attached hereto as **Exhibit 11** is a true and correct copy of the July 1, 2020 *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Microsoft v. John Does 1-2,* Case No. 1:20-cv-00730 (E.D. Va. 2020) (O'Grady, J.).

36. Attached hereto as **Exhibit 12** is a true and correct copy of the July 22, 2020 *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *DXC Technology Company v. John Does 1-2,* Case No. 1:20-cv-00814 (E.D. Va. 2020) (Alston, J.).

37. Attached hereto as **Exhibit 13** is a true and correct copy of the October 6, 2020 *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Microsoft and FS-ISAC v. John Does 1-2,* Case No. 1:20-cv-1171 (E.D. Va. 2020) (Trenga,

J.).

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 26th day of May, 2022.

Garylene Javier