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

MICROSOFT CORPORATION, a Washington corporation, Plaintiff, v. JOHN DOES 1-2 CONTROLLING A COMPUTER NETWORK THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS, Defendants.	Civil Action No: 1:21-cv-822 (RDA/IDD)

DECLARATION OF GABRIEL M. RAMSEY IN SUPPORT OF MICROSOFT'S REQUEST FOR ENTRY OF DEFAULT

I, Gabriel M. Ramsey, declare as follow:

1. I am an attorney admitted to practice in the State of California and the District of Columbia. I am a partner at the law firm of Crowell & Moring LLP, counsel of record for the plaintiff in this matter, Microsoft Corporation ("Microsoft"). I make this declaration in support of Microsoft's Request for Entry of Default. I have personal knowledge of the facts set forth in this declaration and, if called to testify as a witness, could and would testify to the following under oath.

A. Defendants Have Not Responded To This Action Or Otherwise Objected To The Relief Requested In This Action

2. As described more fully below, John Doe Defendants 1-2 ("Defendants") have been properly served the Complaint, and all orders, pleadings and evidence in this action pursuant to the means authorized by the Court in the Temporary Restraining Order (Dkt. 18) and Preliminary Injunction Order (Dkt. 27), and these Defendants have failed to plead or otherwise

defend the action.

3. As of February 22, 2022, I have not been contacted by any of the Defendants regarding this case or at all. I have also conferred with Microsoft, which confirms that neither Microsoft, nor any party associated with it, have been contacted by any of the Defendants regarding this case or at all. I requested that the domain name registrars through which Defendants registered the domains communicate to me if those entities received from Defendants any objection to the Temporary Restraining Order or Preliminary Injunction. Defendants have not conveyed any such communication and Defendants have not otherwise objected to the relief obtained in the Temporary Restraining Order or the Preliminary Injunction Order. Defendants have not objected to or disputed any pleading, declaration, fact, evidence or submission in this case.

4. The 21-day time for Defendants to respond to the complaint under Fed. R. Civ. P. 12 has expired, as Defendants were served on July 22, 2021 and again on November 27, 2021, December 15, 2021 and January 23, 2022, via email and publication and were provided notice of case activities and all pleadings in the case at numerous points between July 22, 2021 and the present via email and publication. Upon information and belief, the Defendants against whom a notation of default is sought are not infants or incompetent persons. I base this conclusion on the fact that Defendants have engaged in sophisticated acts of computer intrusion and theft of sensitive information from computer networks and have operated and procured sophisticated cybercrime infrastructure. I have also seen no indication that Defendants are absent or have failed to file responsive pleadings due to present military service.

B. Service Of Process And Notice Upon Defendants

1. Defendants Are Aware Of This Proceeding Given The Impact Of The TRO And Preliminary Injunction Orders

5. I submit that it is most reasonable to conclude that Defendants are aware of this proceeding given the significant impact of the TRO and preliminary injunction orders on their operations, in combination with the steps Plaintiffs took to serve process by email and through publication, discussed below.

6. As set forth and reflected in Plaintiffs' request for TRO and preliminary injunction, (Dkt. 9, ¶¶ 54-58), following execution of the TRO and preliminary injunction orders, the subject domains that comprised the Defendants' means to carry out theft of information and funds were wholly disabled. As attested, this mechanism was designed to interrupt Defendants' attacks by preventing Defendants from utilizing those domains to target victims. *Id.* Given the obvious impact on the Defendants' infrastructure, I conclude that Defendants are likely to be aware of the impact of the relief granted through the course of this action and to be aware of the fact that the instant proceeding is the cause of that impact, and further aware due to communications from the domain registrars to Defendants regarding the Court order.

C. Service By Internet Publication

7. Plaintiffs' have served process by Internet publication, as authorized by the TRO and Preliminary Injunction Order. The Court found that "[t]here is good cause to permit … service of the Complaint by formal and alternative means… [t]he following means of service of service are authorized by law, satisfy Due Process, and satisfy Fed. R. Ci. P. 4(f)(3) and are reasonably calculated to notify Defendants … of this action: … (2) publishing notice on a publicly available internet website." Dkt. 18 at p. 6, Dkt. 27 at p. 8. The Court has authorized service by Internet publication, as follows: "the Complaint may be served by any means authorized by law, including… publishing notice on a publicly available Internet website." Dkt. 18 at p. 8, Dkt. 27 at p. 10-11.

8. I personally oversaw service of process by publication, including each of the following actions, on behalf of Plaintiffs.

9. Beginning on July 19, 2021, I published the Complaint, TRO and all associated pleadings, declaration and evidence on the publicly available website www.noticeofpleadings.com/maliciousdomains. Thereafter, I published the Preliminary Injunction Order and all other pleadings, declarations, evidence, orders and other submissions filed with the Court in this action on the publicly available website www.noticeofpleadings.com/maliciousdomains. All pleadings and orders filed with the Court have been made available on that website throughout the case.

10. I also included prominently at the top of the website, the following text:

> "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 registrars 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 www.noticeofpleadings.com/maliciousdomains.
>
> 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. COMPLAINT AND SUMMONS

11. A link to the foregoing website was included in each service of process email sent to Defendants at the email addresses determined to be associated with the Defendants' domain

names and associated infrastructure used in the Defendants' operations. Attached hereto as **Exhibit 1** is a true and correct copy of a screenshot of the publicly available website www.noticeofpleadings.com/maliciousdomains.

D. Service By Email

12. Microsoft has served process through email, as authorized by the TRO and Preliminary Injunction Order. The Court has authorized service by email, as follows: "[t]here is good cause to permit … service of the Complaint by formal and alternative means… [t]he following means of service are authorized by law, satisfy Due Process, and satisfy Fed. R. Civ. P. 4(f)(3) and are reasonably calculated to notify Defendants … of this action …(1) transmission by email…" Dkt. 18, ¶ 12, Dkt. 27, ¶ 13. The Court directed that "the Complaint may be served by any means authorized by law, including (1) transmission by email… to the contact information provided by Defendants to Defendants' domain registrars and/or hosting companies and as agreed to by Defendants in the internet domain registration and/or hosting agreements." Dkt. 18 at p. 8, Dkt. 27 at p. 10-11.

13. Through Microsoft's pre-filing investigation, its in-house investigators and attorneys at Crowell & Moring LLP gathered contact information, particularly email addresses, associated with the Defendants' domains. Defendants had provided these email addresses to domain registrars when completing the registration process for the domains used in Defendants' command and control infrastructure. I used this contact information to serve the Defendants by email.

14. In this case, the email addresses provided by Defendants to the domain registrars are the most accurate and viable contact information and means of notice and service. I have personally researched in detail the identifying information and mailing addresses used in the

registration of the domains used by Defendants, as discussed further below. In each case, my investigation has shown that Defendants provided to the domain registrars false or stolen names, addresses, facsimile numbers and telephone numbers. However, in each case Defendants provided an operational, active email address. In some instances, the Defendants registered domains using privacy services that use only the names, addresses, facsimile numbers and telephone numbers of the privacy services. In these cases, an operative email address is provided for the domain privacy service, through which communications may be sent to and pass through to Defendants by the service providers. Defendants will have expected notice regarding their use of the domains by the email addresses that they provided to their domain registrars. ICANN domain registration policies require Defendants to provide accurate email contact information to registrars and the registrars use such information to provide notice of complaints and to send other account-related communications about the domain, including communications which result in suspension or cancellation of the domain registration.

15. Given that Defendants carried out their theft of financial information and significant funds through these domains, it was crucial for them to remain vigilant as to any change of the domains' status, and the email addresses associated with the domains are the means by which they did so. For example, during the course of discovery in this action, I received subpoena responses from the email providers associated with Defendants' email addresses which show that the domain registrars often sent communications, including renewal and billing notices and other communications to Defendants at the email addresses they had provided in association with the domains. Since Defendants were able to maintain the domains active until the execution of this Court's TRO and Preliminary Injunction Order, it follows that Defendants monitored the email accounts to maintain use of the domain registrars' services.

16. I served copies of the Complaint, TRO, Preliminary Injunction Order, and all other pleadings, declarations, evidence, orders and other submissions in this action, by attaching those documents as PDF files to emails sent to the email addresses associated with the domains used by the Defendants. In each such email I included a link to the website www.noticeofpleadings.com/maliciousdomains, at which the pleadings, declarations, evidence and orders filed in this action could also be accessed.

17. I have served the Complaint, TRO, Preliminary Injunction Order, and all other pleadings, declarations, evidence, orders and other submissions in this action, by sending them to the following email addresses used by the Defendants on the following dates. Each of these emails, including notice language, a link to the foregoing public website and including associated attachments, was successfully transmitted to the Defendants:

July 22, 2021	zohoferdz1@gmail.com mbakudgorilla@yahoo.com	Complaint, Temporary Restraining Order Application for TRO and Preliminary Injunction, and all pleadings and evidence in support of the Application for TRO and Preliminary Injunction.
July 26, 2021	zohoferdz1@gmail.com mbakudgorilla@yahoo.com	Motion for Limited Authority to Conduct Doe Discovery, and all pleadings and evidence in support of the Motion. Proposed Preliminary Injunction. Notice of Service of the Complaint and Pleadings re TRO and Preliminary Injunction
July 30, 2021	zohoferdz1@gmail.com mbakudgorilla@yahoo.com	Preliminary Injunction Order Granting Limited Authority to Conduct Doe Discovery
September 24, 2021	zohoferdz1@gmail.com mbakudgorilla@yahoo.com	Notice of Appearance
November 27, 2021	angernrpraving@gmail.com marksincomb26@gmail.com clint1566@gmail.com resultlogg44@gmail.com	Complaint

	zohoferdz1@gmail.com mbakudgorilla@yahoo.com	
December 15, 2021	felorado79@gmail.com angernrpraving@gmail.com marksincomb26@gmail.com clint1566@gmail.com resultlogg44@gmail.com zohoferdz1@gmail.com mbakudgorilla@yahoo.com	Complaint
January 23, 2022	sam@enertrak.co vpickrell@lindsayprecast.co thamric@lindsayprecast.co dwolosiansky@lindsayprecast.co asaxon@martellotech.co felorado79@gmail.com angernrpraving@gmail.com marksincomb26@gmail.com clint1566@gmail.com resultlogg44@gmail.com zohoferdz1@gmail.com mbakudgorilla@yahoo.com	Complaint

18. In each of these emails, I included the following text:

"Plaintiff Microsoft Corporation ("Microsoft") has sued Defendants John Does 1-2 associated with the Internet domains listed in the pleadings attached and set forth at the link 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 registrars 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 www.noticeofpleadings.com/maliciousdomains.

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 this email. 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.

19. Despite this robust notice and service, the Defendants have not contacted me, anyone at my firm, Microsoft, nor any other party associated with Microsoft. Despite notice and service, Defendants have not objected to the relief obtained in the Temporary Restraining Order or the Preliminary Injunction Order. Despite notice and service, Defendants have not objected to or disputed any pleading, declaration, fact, evidence or submission in this case.

E. Attempted Notice And Service By Mail Or Personal Delivery

20. I have investigated each physical mailing address listed in the public registration information associated with the domains used by the Defendants. This information was fabricated by Defendants. To the extent there are particular names listed, I have investigated those as well and determined that they are also fictitious and are aliases by which the Defendants carry out the activities addressed in the Complaint. Across all of the infrastructure investigated during the Doe discovery period, the Defendants persistently utilized two sets of physical address information, which are simply artificial or not associated with Defendants at all.

Robert Chris 3126 Tea Berry Lane Eau Claire WI 54701	There is no such individual associated with this or any address in Eau Claire, WI. This is a fictitious address.
Mbaku Gorilla 1915 Wardrobe Ave Merced, California 95341	There is no such individual associated with this address or any address in Merced, California. This is a real address of a light industrial facility in Merced, California. However, investigation reveals no association with the Defendants.

21. From the foregoing, I conclude that the email addresses associated with the domains and, which are described further above, are the most viable way to communicate with

the Defendants in this action. As noted above, Defendants provided these email addresses when registering the domains used in the command and control infrastructure of their cybercrime operations making it likely that Defendants at least monitor messages sent to those addresses.

F. Microsoft Has Made Substantial, But Unsuccessful, Efforts To Discover And Investigate The Defendants' Particular Identities, Thus The Foregoing Email Information Remains The Best Means To Serve Process In This Case

22. Microsoft endeavored to identify additional contact information through which Defendants could be served, as well as more specific identities. Over the course of its investigation, pursuant to the Court's discovery order, Microsoft has served subpoenas on entities based in the United States in multiple rounds of discovery. Additionally, Microsoft has made inquiries of entities outside of the United States.

23. However, given (a) Defendants' use of aliases and false information, (b) use of anonymous proxy computers or anonymization networks to create and maintain the infrastructure at issue in the case (c) the absence of or limitations on the ability to carry out U.S.-style civil discovery outside of the U.S., (d) the ease with which anonymous activities can be carried out through the Internet and (e) the sophistication of the Defendants in using tools to conceal more specific indicia of their identities or further contact information, I have been unable to specifically and definitively determine the "real" names and physical addresses of Defendants, at which they might be served by personal service.

24. During my investigation of email addresses, I encountered a large number of instances in which Defendants had used free email services. To the extent that I was able to serve subpoenas upon such service providers in the United States, I did so, seeking registration and account information for the free email accounts used by Defendants. I sent similar subpoenas and informal requests to the domain registrars and hosting companies at which the domains were hosted, and received responses. The responses revealed that when registering free

email addresses, and in all records at the registrars and hosting companies, Defendants were able to sign up using fictitious names and contact information.

25. The Defendants also logged into these email accounts, domain registrar accounts and domain hosting accounts from IP addresses that were determined to be proxies. Based on my experience investigating cybercrime matters, I am aware that the sole purpose of such proxy services is to allow Internet users to anonymously use the Internet, without divulging the user's IP address. These proxy computers and services cycle Internet access through a large number of globally distributed IP addresses, thereby concealing the location of the user accessing the Internet through the service. For example, the Internet user's connection to the Internet may be through a first IP address and ordinarily that is what would be displayed when a legitimate user is accessing an email account. However, by using the proxy service, the Defendants' access will reflect the IP address of the proxy computer, rather than the user's actual connection. Often these services "chain" together multiple proxy computers, to make it nearly impossible to trace the original IP address of the user.

26. A handful of IP addresses more directly associated with the Defendants were identified in the records of the infrastructure providers. In each case, these IP addresses were associated with telecommunications companies located in Nigeria. Nigeria is not signatory to the Hague Evidence Convention. Thus, there was no treaty-based means to seek further discovery of these IP addresses.

27. During my investigation I received from email service providers, in response to subpoenas, the email "header information" for emails in the Defendants' account. An email "header" is the section of an email that precedes the message content. It contains the particular routing information of the message, including the sender, recipient, and date. However, it

contains no information about the contents of the email message. In this instance, the email headers showed that Defendants were obtaining services from certain other service providers, including hosting providers and domain registrars. The header information indicated that Defendants were testing domains for use in the activities set forth in the Complaint. I sent subpoenas to these companies, but the information in their possession regarding Defendants was all falsified identities or IP addresses that did not reveal Defendants' actual identities or locations.

28. I also attempted to investigate Defendants' identities through the means of payment for the relevant domains. Defendants paid for their infrastructure using either the cryptocurrency Bitcoin or an alternative digital currency called Perfect Money, both of which allow Defendants to anonymously purchase infrastructure, including the domains at issue. Defendants' means of payment did not reveal Defendants' actual identities or locations.

29. I have carried out every reasonable effort and have used every tool, technique and information source available to me to further specifically identify Defendants' true identities and physical locations. I conclude that I have exhausted my ability to investigate Defendants' true identities using civil discovery tools, despite my best efforts and the exercise of reasonable diligence to determine Defendants' identities.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct to the best of my knowledge. Executed on this 22nd day of February, 2022, in San Francisco, California.

Gabriel M. Ramsey

CERTIFICATE OF SERVICE

I hereby certify that on February 23, 2022, I will electronically file the foregoing with the Clerk of Court using the CM/ECF system.

Copies of the foregoing were also served on the defendants listed below by electronic mail:

John Does 1-2

c/o

sam@enertrak.co
vpickrell@lindsayprecast.co
thamric@lindsayprecast.co
dwolosiansky@lindsayprecast.co
asaxon@martellotech.co
felorado79@gmail.com
angernrpraving@gmail.com
marksincomb26@gmail.com
clint1566@gmail.com
resultlogg44@gmail.com
zohoferdz1@gmail.com
mbakudgorilla@yahoo.com

/s/ David J. Ervin

David J. Ervin (VA Bar No. 34719)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Telephone: (202) 624-2500
Fax: (202) 628-5116
dervin@crowell.com

Attorneys for Plaintiff Microsoft Corp.