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 AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS, Defendants.	Civil Action No: 1:22-cv-607-AJT-WEF

DECLARATION OF GABRIEL M. RAMSEY IN SUPPORT OF PLAINTIFF'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. I am a partner at the law firm of Crowell & Moring LLP, counsel of record for the plaintiff in this matter, Microsoft Corporation ("Microsoft") ("Plaintiff"). I make this declaration in support of Plaintiff'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, summons, and all orders, pleadings and evidence in this action pursuant to the means authorized by the Court in the Temporary Restraining Order (Dkt.

16) and Preliminary Injunction Order (Dkt. 24), and these Defendants have failed to plead or otherwise defend the action.

3. As of May 1, 2023, 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. Defendants have not objected to the relief obtained in the Temporary Restraining Order or the Preliminary Injunction Order, or any other order of the Court. 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 June 2, 2022 and again on June 8, 2022 via email and publication and were provided notice of case activities at numerous points from June 2, 2022 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 on their operations, in combination with the steps Plaintiff took to serve process by email and through publication, discussed below.

6. As set forth and reflected in Plaintiff's request for TRO and request for preliminary injunction, following execution of these orders, the subject domain names that comprised the Defendants' command and control infrastructure to target victims, gain unauthorized access to their accounts and information and infect victim operating systems and devices, was disabled. As attested, this mechanism was designed to interrupt Defendants' attacks by removing infrastructure used to deceive victims of phishing emails and severing communications between the infected operating systems and devices of victims and the Defendants. *See, e.g.*, Declaration of Christopher Coy ISO Microsoft's Applications For An Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause re Preliminary Injunction (Dkt. 8-5), ¶¶ 38-42. Accordingly, I believe that this effectively interrupted Defendants' attacks by severing communications between the infected operating systems and devices. Given this disruption and impact on the Defendants' infrastructure, , I conclude that Defendants are very 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.

C. Service By Internet Publication

7. Plaintiff has served process by Internet publication, as authorized by the TRO and Preliminary Injunction Order. 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. 16 at p. 10.

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

9. Beginning on June 2, 2022, I published the Complaint, summons, TRO and all associated pleadings, declaration and evidence on the publicly available website

www.noticeofpleadings.com/Bohrium. 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/Bohrium. 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 domains listed in the documents set forth herein. Plaintiff alleges that Defendants have violated Federal and state law by hosting a cybercriminal operation through these domains, causing unlawful intrusion into Plaintiff customers' computers and computing devices and intellectual property violations to the injury of Plaintiff's customers. Plaintiff seeks a preliminary injunction directing the domain registrars and registries associated with these domains to take all steps necessary to disable access to and operation of these domains to ensure that changes or access to the domains cannot be made absent a court order and that all content and material associated with these domains are to be isolated and preserved pending resolution of the dispute. Plaintiff seeks a permanent injunction, other equitable relief and damages. Full copies of the pleading documents are available at www.noticeofpleadings.com/Bohrium. 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 Microsoft's attorney, Gabriel M. Ramsey at Crowell & Moring, LLP, 3 Embarcadero Center, 26th Floor, San Francisco, CA 94111. If you have questions, you should consult with your own attorney immediately."

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 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/Bohrium.

D. Service By Email

12. Plaintiff has served process through email, as authorized by the TRO, and Preliminary Injunction Order. The Court has authorized service by email, as follows: "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 domain registration and/or hosting agreements." Dkt. 16 at p. 10.

13. Through Plaintiff's pre-filing investigation and through the Doe discovery process in this case, Plaintiff's in-house investigators and attorneys at Crowell & Moring LLP gathered contact information, particularly email addresses, associated with the Defendants' domain names. Defendants had provided these email addresses to domain registrar companies when completing the registration process for the domain names 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 domain names 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 to the domain registrars. Defendants will have expected notice regarding their use of the domain names by the email addresses that they provided to their domain registrars. For example, as set forth in the Declaration of Garylene Javier at Dkt. 8-2 ¶¶ 8, 18-29, domain registrar policies require Defendants to provide accurate email contact information to domain registrars to use such information to provide notice of complaints and to send other account-related communications about the domain names, including communications which result in suspension or cancellation of the domain names.

15. Given that Defendants relied upon these domain names to deceive users, to obtain unauthorized access to victim accounts and victim data, and to connect to victim computers infected with malware, it was crucial for them to remain vigilant as to any change of the domain names' status, and the email addresses associated with the domain names are the means by which they did so. For example, during the course of discovery in this action, I received subpoena responses from domain registrars associated with Defendants' email addresses which show that the domain registrars often sent communications, including registration, renewal and billing notices and other communications to Defendants at the email addresses they had provided in association with the domain names. Since Defendants were able to maintain the domain names active until the execution of this Court's TRO or 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 domain names used by the Defendants. In each such email I included a link to the website www.noticeofpleadings.com/Bohrium, 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:

shashankvashist8@gmail.com
proxy@whoisprotectservice.com
a1608ba6e3474ec39c199d7393d6197c.protect@withheldforprivacy.com
c9cd38cd98544330b9d1ee01d2274c51.protect@withheldforprivacy.com
pw-a60513b92fbdf8a76f7992b8aeeae8bd@privacyguardian.org
jatin.hariani2@gmail.com

2718c72e76ca4c9fbef4b8519e55fa82.protect@withheldforprivacy.com
sitesanalyzer.com-registrant@directnicwhoiscompliance.com
a37d251531904cd69d7b8a18f3a3e933.protect@withheldforprivacy.com
jatin.hariani2019@protonmail.com
pw-444878576c12808ba2d6242daa9219ed@privacyguardian.org
1bc09a1d8a5240558bf84382c0e5725f.protect@withheldforprivacy.com
pw-4d4e978a1b05a4d5140ea4fb59f6f46a@privacyguardian.org

In connection with sending the emails, I used a service called ReadNotify to track the email correspondence. By appending ".readnotify.com" to the end of each of the registrant emails, I was able to track the correspondence, including when the emails were received and opened. Each of the foregoing emails were opened.

18. In particular, on June 2, 2022, I served the Defendants by sending an email to Defendants' attaching the Complaint and TRO, and the foregoing link to all other pleadings, documents and orders in the case. In these initial emails that I sent to Defendants, I included the following text:

> Plaintiff Microsoft Corporation ("Microsoft"), has sued Defendants John Does 1-2 associated with the domains listed in the documents set forth herein. Plaintiff alleges that Defendants have violated Federal and state law by hosting a cybercriminal operation through these domains, causing unlawful intrusion into Plaintiff customers' computers and computing devices and intellectual property violations to the injury of Plaintiff's customers. Plaintiff seeks a preliminary injunction directing the domain registrars and registries associated with these domains to take all steps necessary to disable access to and operation of these domains to ensure that changes or access to the domains cannot be made absent a court order and that all content and material associated with these domains are to be isolated and preserved pending resolution of the dispute. Plaintiff seeks a permanent injunction, other equitable relief and damages. Full copies of the pleading documents are available at www.noticeofpleadings.com/Bohrium. 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 Microsoft's attorney, Gabriel M. Ramsey at Crowell & Moring, LLP, 3 Embarcadero Center, 26th Floor, San Francisco, CA 94111. If you have questions, you should consult with your own attorney immediately."

19. Thereafter, I sent copies of all other briefs, submissions and orders on the docket in this matter, along with a link to www.noticeofpleadings.com/Bohrium at which the complaint

and all documents in this matter are readily available. 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, the Preliminary Injunction Order, or any other order in the case. 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 information associated with the domain names used by the Defendants and in the records regarding those domain names obtained during discovery. This information was fabricated by Defendants. These addresses reflected: (1) incomplete addresses, such as only the names of cities without further detail, (2) addresses that are simply artificial and do not exist at all, (3) street names that exist but not properly correlated to other address information and associated with individuals or companies that do not exist, and (4) city names that are not properly correlated to the listed country or which combine elements of different cities in different countries.

21. From the foregoing, I conclude that the email addresses associated with the domain names 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 domain names 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. Plaintiff 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. On behalf of Plaintiff, I endeavored to identify additional contact information

through which Defendants could be served, as well as more specific identities. Over the course of Plaintiff's investigation, pursuant to the Court's discovery order, I served thirteen subpoenas to the U.S.-based domain registrars, waited for responses and analyzed the responses, in an effort to obtain additional information regarding Defendants' identities. The rest of the domain registrars at issue were located outside of the U.S., outside of the reach of civil discovery, as were hosting companies upon which Defendants hosted content associated with the domains. Thus, the domain registrars represented the only viable leads to pursue via discovery or informal means.

23. Analysis of login IP address information used for all discoverable infrastructure revealed that Defendants used sophisticated techniques and services to conceal their actual IP address and location, and to proxy their communications through third-party computers. In other words, the login IP addresses were only associated with intermediary computers that could not be traced to the Defendants. Thus, it has not been possible to identify Defendants with any greater particularity through these means either.

24. 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.

25. 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 1st day of May, 2023 in San Francisco, California.

Gabriel M. Ramsey

CERTIFICATE OF SERVICE

I hereby certify that on May 2, 2023, I will electronically file the foregoing with the Clerk of Court using the CM/ECF system. Copies of the forgoing were also served on the defendants listed below by electronic mail:

John Does 1-2 c/o

shashankvashist8@gmail.com
proxy@whoisprotectservice.com
a1608ba6e3474ec39c199d7393d6197c.protect@withheldforprivacy.com
c9cd38cd98544330b9d1ee01d2274c51.protect@withheldforprivacy.com
pw-a60513b92fbdf8a76f7992b8aeeae8bd@privacyguardian.org
jatin.hariani2@gmail.com
2718c72e76ca4c9fbef4b8519e55fa82.protect@withheldforprivacy.com
sitesanalyzer.com-registrant@directnicwhoiscompliance.com
a37d251531904cd69d7b8a18f3a3e933.protect@withheldforprivacy.com
jatin.hariani2019@protonmail.com
pw-444878576c12808ba2d6242daa9219ed@privacyguardian.org
1bc09a1d8a5240558bf84382c0e5725f.protect@withheldforprivacy.com
pw-4d4e978a1b05a4d5140ea4fb59f6f46a@privacyguardian.org

Dated: May 2, 2023

Respectfully submitted,

/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