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: 1:19-cv-01582 (LO/JFA)

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. 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, summons, and all orders, pleadings and evidence in this action pursuant to the means authorized by the Court in the Temporary Restraining Order (Dkt. 19) and Preliminary Injunction Order (Dkt. 28), and these Defendants have failed to plead or

otherwise defend the action.

3. As of August 23, 2020, I have not been contacted by any of the Defendants regarding this case or at all. I have also conferred with Richard Boscovich, Assistant General Counsel in Microsoft's Digital Crimes Unit, who 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 order of the Court Monitor. 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 December 24, 2019 via email and publication and at numerous points between December 2019 and June 2020 via email. 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 Microsoft took to serve process by email and through publication, discussed below.

6. As attested in the Declaration of David Anselmi (Dkt. 14 ¶¶ 35-37), following execution of the TRO and preliminary injunction orders, traffic from the subject Internet domains that comprised the Defendants' command and control infrastructure to infected victim operating systems and devices, was redirected to Microsoft's secure servers. As attested, this mechanism was designed to interrupt Defendants' attacks by severing communications between the infected operating systems and devices of at least 122 victims and the Defendants. *Id.* Given the obvious impact on the infrastructure, I conclude that Defendants are very likely to be aware of that impact and to be aware of the fact that the instant proceeding is the cause of that impact.

C. Service By Internet Publication

7. Microsoft has served process by Internet publication, as authorized by the TRO, Preliminary Injunction Order and Supplemental 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. 19 at p. 10.

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

9. Beginning on December 23, 2019, I published the Complaint, summons, TRO and all associated pleadings, declaration and evidence on the publicly available website www.noticeofpleadings.com/thallium. 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/thallium. 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 below. Microsoft alleges that Defendants have violated Federal and state law by hosting a cybercriminal operation through these Internet domains, causing unlawful intrusion into Microsoft and Microsoft's customers' computers and computing devices; 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 these Internet domains to ensure that changes or access to the Internet domains cannot be made absent a court order and that all content and material associated with these Internet domains 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/thallium.
>
> 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' domains used in the Thallium operations. Attached hereto as **Exhibit 1** is a true and correct copy of a screenshot of the publicly available website www.noticeofpleadings.com/thallium.

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: "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." Dkt. 19 at p. 10.

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 to the domain registrars. Defendants will have expected notice regarding their use of the domains by the email addresses that they provided to their domain registrars. For example, as set forth in the Declaration of Kayvan Ghaffari at Dkt. 15 ¶¶ 15-31, 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 connected to the infected victim computers 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 Thallium Defendants. In each such email I included a link to the website www.noticeofpleadings.com/thallium, 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:

tang_guanghui@hotmail.com
bitcoin024@hanmail.net
bitcoin025@hanmail.net
satoshiman0088@gmail.com
noreplygooqlesender@gmail.com
pigcoin2020@hotmail.com
rninchurl@daum.net
tiger199392@daum.net
infornail.noreply@gmail.com
jiahuzong@hotmail.com
wusongha03@gmail.com
23f30d8e5ab4439fb15be24a7de1ffb8.protect@whoisguard.com
okonoki_masao@yahoo.co.jp

18. In particular, on December 24, 2019, I served the Defendants by sending an email to Defendants' attaching the Complaint, 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 Internet domains listed in the attached Complaint and Temporary Restraining Order. Microsoft alleges that Defendants have violated Federal and state law by hosting a cybercriminal operation through these Internet domains, causing unlawful intrusion into Microsoft and Microsoft's customers' computers and computing devices; 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 these Internet domains to ensure that changes or access to the Internet domains cannot be made absent a court order and that all content and material associated with these Internet domains 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/thallium.
>
> 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. On January 12, 2020, I served the Preliminary Injunction Order, by sending an email attaching that order to the Defendants, and again including the foregoing language.

20. On June 6, 2020, I served all of the foregoing documents and the foregoing language on an additional email address that was identified during the course of discovery.

hello-0978@daum.net

21. 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, and 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.

22. I used an email tracking service to monitor whether the service emails that I sent

to Defendants were opened. The service reported that the emails were opened by Defendants on the following dates and times:

December 25, 2019 at 00:14:50am (UTC -7:00)	December 25, 2019 at 00:18:36am (UTC -7:00)
December 25, 2019 at 00:15:37am (UTC -7:00)	December 25, 2019 at 00:17:38am (UTC -7:00)
January 12, 2020 at 22:03:09pm (UTC -7:00)	January 12, 2020 at 22:03:14pm (UTC -7:00)
January 12, 2020 at 22:05:33pm (UTC -7:00)	

E. Attempted Notice And Service By Mail Or Personal Delivery

23. I have investigated each physical mailing address listed in the public registration information associated with the domains used by the Defendants and in the records regarding those domains 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 companies that do not exist, and (4) city names that are not properly correlated to the listed country.

24. 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

25. On behalf of Microsoft, I 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, I served six subpoenas to six domain

registrars and hosting companies, waited for responses and analyzed the responses, in an effort to obtain additional information regarding Defendants' identities. Based on information obtained during the initial waves of discovery, I sent further subpoenas and informal discovery requests to additional hosting companies, until there were no further viable leads to pursue via discovery or informal means.

26. These discovery efforts yielded various names, addresses and credit card numbers. Further investigation revealed that the names, addresses, and credit card information used by Defendants were fake or stolen. Defendants also made numerous payments using anonymous Bitcoin payments that are not associated with any particular identity.

27. I identified several hosting companies involved with Defendants' infrastructure and from discovery to those sources learned and examined IP addresses used to create, host and log into that relevant infrastructure. Defendants, however, used sophisticated techniques and services designed to conceal their actual IP address and location, and to proxy their communications through third-party computers. Thus, it has not been possible to identify Defendants with any greater particularity through these means either.

28. 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.

29. During my investigation of email addresses, I encountered only instances in which Defendants had used free email services in jurisdictions which have no reciprocal discovery means with the United States. During my investigation of domain and hosting account information, I discovered that the Defendants logged into these 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.

30. In particular, my investigation revealed that Defendants used anonymous VPN services or networks and/or the "The Onion Router" (aka "Tor") networks, which are collectively designed to and have the effect of concealing the source IP address by encrypting the traffic and routing it through multiple, random intermediate computers. I determined this by either looking up the IP addresses in publicly available repositories of known Tor nodes, or by sending subpoenas and informal requests to the operators of the IP addresses and receiving responses that they were such nodes. The result is that login IP addresses seen in email account, registrar and hosting company records are from random intermediate machines in scores of countries (and given the operation of anonymous VPN and Tor, those intermediate machines

often have numerous other intermediate machines between the login IP and Defendants' ultimate source IP). Thus, Defendants were able to conceal their identities, source IP addresses and physical locations.

31. 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 23rd day of August, 2020, in San Francisco, California.

Gabriel M. Ramsey

EXHIBIT 1

Date of First Publication: December 23, 2019

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: 1:19-cv-1582

Plaintiff Microsoft Corporation ("Microsoft") has sued Defendants John Does 1-2 associated with the Internet domains listed below. Microsoft alleges that Defendants have violated Federal and state law by hosting a cybercriminal operation through these Internet domains, causing unlawful intrusion into Microsoft and Microsoft's customers' computers and computing devices; 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 these Internet domains to ensure that changes or access to the Internet domains cannot be made absent a court order and that all content and material associated with these Internet domains 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/thallium (http://www.noticeofpleadings.com/thallium).

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.

COMPLAINT AND SUMMONS

Complaint (http://noticeofpleadings.com/thallium/files/FINAL COMPLAINT.pdf)

Civil Cover Sheet (http://noticeofpleadings.com/thallium/files/Civil Cover Sheet.pdf)

COURT ORDERS

Order Granting TRO and Order to Show Cause re PI (http://noticeofpleadings.com/thallium/files/Order Granting TRO and Order to Show Cause re PI.pdf)

Order Granting Motion to Seal (http://noticeofpleadings.com/thallium/files/Order Granting Motion to Seal.pdf)

Order Unsealing Docket for Good Cause Shown (http://noticeofpleadings.com/thallium/files/Order Granting TRO and Order to Show Cause re PI.pdf)

Order Granting Preliminary Injunction (http://noticeofpleadings.com/thallium/files/2020.01.03 ECF 28 Preliminary Injunction Order.pdf)

Order Unsealing Docket (http://noticeofpleadings.com/thallium/files/2019.12.27 ECF 25 Order Unsealing Docket for Good Cause Shown.pdf)

APPLICATION FOR EMERGENCY TEMPORARY RESTRAINING ORDER (TRO) AND PRELIMINARY INJUNCTION

Application for TRO and Preliminary Injunction (http://noticeofpleadings.com/thallium/files/Application for TRO and Preliminary Injunction.pdf)

Brief In Support of Motion for TRO and Preliminary Injunction (http://noticeofpleadings.com/thallium/files/Brief In Support of Motion for TRO and Preliminary Injunction.pdf)

Proposed Order re TRO and Preliminary Injunction (http://noticeofpleadings.com/thallium/files/Proposed Order re TRO and Preliminary Injunction.pdf)

Anselmi Declaration in Support of Motion for TRO and Preliminary Injunction (http://noticeofpleadings.com/thallium/files/Anselmi Declaration in Support of Motion for TRO and Preliminary Injunct....pdf)

Ghaffari Declaration in Support of Motion for TRO and Preliminary Injunction (http://noticeofpleadings.com/thallium/files/Ghaffari Declaration in Support of Motion for TRO and Preliminary Injunc.pdf)

MOTION FOR ORDER TEMPORARILY SEALING DOCUMENTS

Motion to Seal (http://noticeofpleadings.com/thallium/files/Motion to Seal.pdf)

Brief in Support of Motion to Seal Documents (http://noticeofpleadings.com/thallium/files/Brief in Support of Motion to Seal Documents.pdf)

Ramsey Declaration in Support of Motion to Seal Document (http://noticeofpleadings.com/thallium/files/Ramsey Declaration in Support of Motion to Seal Document.pdf)

Proposed Order re Motion to Seal (http://noticeofpleadings.com/thallium/files/Proposed Order re Motion to Seal.pdf)

December 23, 2019 Notice of Execution of Ex Parte Temporary Restraining Order and Notice re Unsealing of Case (http://noticeofpleadings.com/thallium/files/December 23, 2019 Notice of Execution of Ex Parte Temporary Restraining ....pdf)

MOTION FOR DOE DISCOVERY

Motion for Doe Discovery (http://noticeofpleadings.com/thallium/files/2020.01.13 ECF 29 Motion for Doe Discovery.pdf)

Brief in Support of Motion for Doe Discovery (http://noticeofpleadings.com/thallium/files/2020.01.13 ECF 30 Brief ISO Motion for Doe Discovery.pdf)

Proposed Order in Support of Motion for Doe Discovery (http://noticeofpleadings.com/thallium/files/2020.01.13 ECF 31 Proposed Order.pdf)

Notice of Hearing on Motion for Doe Discovery (http://noticeofpleadings.com/thallium/files/2020.01.13 ECF 32 Notice of Hearing Date re Doe Discovery Motion.pdf)

NOTICES

Notice of Execution (http://noticeofpleadings.com/thallium/files/2019.12.23 ECF 24 Notice of Execution of Temporary Restraining Order and Motion to Unseal.pdf)

MISCELLANEOUS

Bond Check (http://noticeofpleadings.com/thallium/files/2019.12.23 ECF 23 Bond Check.pdf)

Contact Us

If you wish to contact us by e-mail, fax, phone or letter please contact us at:

Gabriel Ramsey
Crowell & Moring LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111

Telephone: +1 (415) 365-7207
Facsimile: +1 (415) 986-2827
Email: gramsey@crowell.com (mailto:gramsey@crowell.com)