**UNITED STATES DISTRICT COURT**
**SOUTHERN DISTRICT OF NEW YORK**

| | | |
|---|---|---|
| MICROSOFT CORPORATION, | : | |
| | : | |
| Plaintiff, | : | **Case No.** |
| -against- | : | |
| | : | |
| DUONG DINH TU, | : | **JURY TRIAL DEMANDED** |
| LINH VAN NGUYEN, and | : | |
| TAI VAN NGUYEN, | : | **REQUEST TO FILE UNDER SEAL** |
| | : | |
| Defendants. | : | |

---

**DECLARATION OF JASON ROZBRUCH IN SUPPORT OF PLAINTIFF MICROSOFT'S MOTION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE**

---

I, Jason Rozbruch, declare as follows:

1. I am an attorney with the law firm of Cahill Gordon & Reindel LLP ("Cahill") and am counsel for Plaintiff Microsoft Corporation ("Microsoft") in the above-captioned action. I make this declaration in support of Microsoft's Motion for an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause ("TRO Motion"). Unless otherwise noted, the facts set forth below are based on my personal knowledge or upon information and belief on the basis of my review of evidence collected as part of Microsoft's investigation in this case.

## I. Parties

2. Plaintiff Microsoft seeks an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause to disable specified Internet domains that are being used by Defendants Duong Dinh Tu, Linh Van Nguyen (a/k/a Nguyen Van Linh), and Tai Van Nguyen ("Defendants") to operate a sophisticated Internet-based criminal operation referred to herein as the "Fraudulent

Enterprise" (or the "Enterprise"). The Fraudulent Enterprise specializes in selling fraudulently-procured Microsoft accounts in bulk to cybercriminals who then use the accounts for various types of cybercrime activity, wreaking havoc on Microsoft and its customers.

3. As counsel of record for Plaintiff, I am aware of previous efforts by Microsoft 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; the "Trickbot" threat infrastructure in October 2020 in the Eastern District of Virginia; the "ZLoader" threat infrastructure in April 2022 in the Northern District of Georgia; and the "Cobalt Strike" threat infrastructure in March 2023 in the Eastern District of New York.

4. As part of my involvement in the investigation in this case, I have learned about Microsoft's prior experiences litigating claims against cybercrime defendants who conduct their operations using technological infrastructure consisting of a set of websites, domains, and Internet protocol ("IP") addresses. Based Microsoft's prior experiences in such matters, I believe and

respectfully submit that the request *ex parte* relief is necessary here, 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 prosecution of this matter futile.

5. For example, I am aware that in an earlier matter in which Microsoft attempted 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. Likewise, I understand that 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 a court-approved temporary restraining order. Moreover, during a prior action regarding the ZeroAccess Botnet in November 2013, the operators of that botnet immediately attempted (unsuccessfully) to act, in response to the seizure of domains to attempt to move the botnet's command and control infrastructure. Based on these and other prior experiences of Microsoft, I believe and respectfully submit that there is a similar risk that Defendants here would take similar actions to evade or obstruct a temporary restraining order in this case.

6. Microsoft's counsel has not attempted to provide notice of the TRO Motion to Defendants, and I respectfully submit should not be required to provide notice at this time. I respectfully submit that good and sufficient reasons exist for this TRO Motion to be made by Order to Show Cause in lieu of by notice of motion. Microsoft has previously sought and received *ex parte* temporary restraining orders in a number of federal district courts in prior cases, including: *Microsoft Corporation and FSISAC, Inc.* v. *John Does 1-2*, Case No. 20 Civ. 1171 (E.D. Va. 2020)

(Trenga, J.); *Microsoft Corporation et al.* v. *Malikov and John Does 1-7*, Case No. 22 Civ. 01328 (N.D. Ga.) (Cohen, J.); *Microsoft Corp. et al.* v. *John Does 1-2 et al.*, Case No. 23 Civ. 02447 (E.D.N.Y. 2023) (Morrison, J.). Microsoft, however, has not previously sought *ex parte* relief in this District or as to these particular Defendants.

7. Plaintiff has identified certain Internet domains that are believed to be part of the infrastructure used by the Defendants' Fraudulent Enterprise. The domains associated with Defendants' infrastructure are set forth in Appendix A to Plaintiff's proposed Complaint in this case. A true and correct copy of Appendix A to the Complaint is attached hereto as Exhibit 1.

8. I understand that investigators of Microsoft's Digital Crimes Unit and of Arkose Labs, including declarants in this action, have worked to determine the true identities of Defendants. Based on my own research and based on Digital Crimes Unit's research regarding these domains, the WHOIS information associated with these domains is not public and the only way to make contact with Defendants are the registrant email contact facilities provided by the domain registrars and the email addresses provided by Defendants to the Internet domain name registrars during the domain name registration and maintenance process.[1] This information may further include individual and entity names, physical addresses, email addresses, facsimile numbers, and telephone numbers, which can only be obtained through a court order or subpoena.

9. To the extent Defendants have provided such information, the information most likely to be accurate are e-mail addresses as, upon information and belief, such are necessary to register Internet domains and associated infrastructure. It is more likely that the email addresses

[1] Through its investigation, Microsoft has uncovered several email addresses that, upon information and belief, it asserts belong to the three named Defendants. Cahill, on behalf of Microsoft, will seek to effectuate notice to these email addresses: "duongdinhtu93@gmail.com," "duongdinhtu93@outlook.com," "17021195@vnu.edu.vn," "nguyenlinh.uet@gmail.com," and "nvt.kscntt@gmail.com."

exist and are functional than it is likely that the personal names and physical addresses are correct or accurate. I believe 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 and associated IP addresses. Other contact information, such as physical address information, is more likely to be false. I base this conclusion, in part, on my knowledge of past experiences relating to cybercrime in which domain or IP address 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."

10. Based on my knowledge of 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 or IP addresses, and the contact information, particularly email addresses, in possession of the Internet domain registrars or hosting companies. From my research, I believe that such contact information is likely to be valid, as it is necessary to obtain Internet domain names or web hosting services. 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, aside from the email addresses provided above, 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 discovery, these companies will be unlikely to share contact information that would allow Microsoft to provide notice and service to Defendants.

## II. Notice and Service of Process

### A. Microsoft has Robust Plans to Provide Notice

11. On behalf of Microsoft, Cahill will attempt notice of any 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 IP address hosting companies. Cahill will send such documents to the email addresses of Defendants Duong Dinh Tu ("duongdinhtu93@gmail.com" and "duongdinhtu93@outlook.com"), Linh Van Nguyen (a/k/a Nguyen Van Linh) ("17021195@vnu.edu.vn" and "nguyenlinh.uet@gmail.com"), and Tai Van Nguyen ("nvt.kscntt@gmail.com").

12. On behalf of Microsoft, Cahill will attempt notice of any preliminary injunction hearing and service of the Complaint by publishing those pleadings on a publicly accessible website located at: https://dcu-noticeofpleadings.azurewebsites.net/. Cahill 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 Duong Dinh Tu, Linh Van Nguyen (a/k/a Nguyen Van Linh), and Tai Van Nguyen, who are associated with the Internet domains set forth in the documents referenced in this communication. Microsoft alleges that Defendants have violated Federal and state law by

> hosting a cybercriminal operation through these Internet domains, causing unlawful deception of and intrusion into Microsoft's computer systems; 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 transfer these Internet domains to Microsoft's control and/or disable access to and operation of these 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 final judgment and permanent injunction, other equitable relief and damages. Full copies of the pleading documents are available at https://dcu-noticeofpleadings.azurewebsites.net/.

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 Microsoft's attorneys, attention to Jason Rozbruch, 32 Old Slip, 19th Floor, New York, NY 10005. If you have questions, you should consult with your own attorney immediately.

13. On behalf of Microsoft, Cahill will serve each of the third parties identified in Microsoft's [Proposed] Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause with copies of all documents served on Defendants.

14. On behalf of Microsoft, Cahill will also attempt notice of any 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.

15. On behalf of Microsoft, Cahill will prepare Requests for Service Abroad of Judicial or Extrajudicial Documents to attempt notice of any 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, Cahill 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 any 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**

16. 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.

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

18. 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**

19. 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, email 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[.]

20. 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**

21. 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.

22. 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.

23. 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.

24. Pursuant to the Rules, notice of a complaint may be achieved by the registrar forwarding the complaint to the postal address, facsimile number and email 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[.]

25. 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**

26. 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**

27. 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.

28. 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**

29. 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. For example, Public Domain Registry's ("Public Domain") Registrar-Registrant Terms of Service, available at https://publicdomainregistry.com/legal/#tos, include such provisions. A true and correct copy of Public Domain's Domain Name Registration Terms of Service attached hereto as Exhibit 7.

30. Based on my research of third parties that Defendants use to provide domain name services, the other third party Internet hosting companies and 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**

31. 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, Public Domain's agreement prohibits, among other conduct, the registered domain being used to:

a. distributing malware or other malicious code;

b. hosting or linking to a website intended to deceive the public;

c. infringing upon the Intellectual Property Rights of Others;

d. purposely send out mass spams like mass unsolicited, commercial advertising or solicitations and so on;

e. send out retroactive, pornographic or other harmful emails that violate the country laws and rules;

f. Accessing another network without permission, to probe or scan for vulnerabilities or breach security or authentication measures;

g. Attacking other networks (*i.e.*, Denial of Service (DoS) attacks);

h. Intercepting or monitoring data without permission;

i. Running a file sharing site;

j. Running any software that interfaces with an IRC (Internet Relay Chat) network;

k. Using any deep-link, page-scrape, robot, crawl, index, spider, offline reader, click spam, macro programs, internet agent, or other automatic device, program, algorithm or methodology which does the same things, to use, access, copy, index, acquire information, generate impressions or clicks, input information, store information, search, generate searches, or monitor any portion of our website or servers for any unauthorized purpose;

l. resolve, point or forward to the website with harmful information that violate the country laws and rules; or

m. engage in other illegal actions.

32. Public Domain'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 knowledge of prior experience and my current research of other Internet domain registrars and hosting companies, and on information and belief, the other Internet domain registrars and hosting companies used by Defendants prohibit similar unlawful conduct.

## III. OTHER AUTHORITY AND EVIDENCE

33. Attached hereto as Exhibit 8 is a true and correct copy of the March 31, 2023 *Ex Parte* Temporary Restraining Order and Order to Show Cause (ECF 13) in the matter of *Microsoft Corp. et al.* v. *John Does 1-2 et al.*, Case No. 23 Civ. 02447 (E.D.N.Y. 2023).

34. Attached hereto as Exhibit 9 is a true and correct copy of the March 5, 2020 *Ex Parte* Temporary Restraining Order and Order to Show Cause (ECF 11) in the matter of *Microsoft Corp.* v. *John Does 1-2*, Case No. 20 Civ. 1217 (E.D.N.Y. 2020).

35. 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 (ECF 15) in the matter of *Sophos* v. *John Does 1-2*, Case No. 20 Civ. 00502 (E.D. Va. 2020).

36. 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 (ECF 15) in the matter of *Microsoft* v. *John Does 1-2*, Case No. 20 Civ. 00730 (E.D. Va. 2020).

37. 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 (ECF 13) in the matter of *DXC Technology Company* v. *John Does 1-2*, Case No. 20 Civ. 00814 (E.D. Va. 2020).

38. Attached hereto as Exhibit 13 is a true and correct copy of the December 7, 2021 *Ex Parte* Temporary Restraining Order and Order To Show Cause (ECF 8) in the matter of *Google LLC* v. *Starovikov, et al.*, Case No. 21 Civ. 10260 (S.D.N.Y. 2021).

39. Attached hereto as Exhibit 14 is a true and correct copy of Microsoft's Annual Report 2023, which is also available at https://www.microsoft.com/investor/reports/ar23/index.html.

I declare under penalty of perjury of the laws of the United States of America that the foregoing is true and correct.

Executed on this 7th day of December, 2023 in New York, New York.

Jason Rozbruch