UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MICROSOFT CORP.,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING COMPUTER BOTNETS AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS,

Defendants.

Case No. 20-CV-1217 (LDH)

PRELIMINARY INJUNCTION ORDER

Plaintiff Microsoft Corporation ("Microsoft") has filed a complaint for injunctive and other relief pursuant to: (1) The Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) Electronic Communications Privacy Act, 18 U.S.C. § 2701; (3) Trademark Infringement under the Lanham Act, 15 U.S.C. § 1114 *et seq*. (4) False Designation of Origin under the Lanham Act, 15 U.S.C. § 1125(a); (5) Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c); (6) common law trespass to chattels; (7) conversion; (8) unfair competition; and (9) unjust enrichment. Microsoft has moved *ex parte* for an emergency temporary restraining order and an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C. § 1116(a) (the Lanham Act), and 28 U.S.C. § 1651(a) (the All-Writs Act). On March 5, 2020, the Court issues a temporary restraining order and order to show cause why an injunction should not issue ("March 5, 2020 Temporary Restraining Order"). Defendants have not responded to the Court's order to show cause.

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Microsoft's request for a Preliminary Injunction, and having heard oral argument on March 31,

2020, the Court hereby makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case, and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against Defendants John Does ("Defendants") under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), CAN-SPAM Act (15 U.S.C. § 7704), and common law of trespass to chattels, unjust enrichment, conversion, and intentional interference with contractual relationships.

2. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), and constitute common law of trespass to chattels, unjust enrichment, conversion, and intentional interference with contractual relationships, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. Microsoft owns the registered trademarks "Microsoft," "Windows," and numerous other trademarks used in connection with its services, software and products. There is good cause to believe that, unless Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations. The evidence set forth in Microsoft's Brief in Support of *Ex Parte* Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Application"), and the accompanying declarations and exhibits, demonstrates that Microsoft is likely to prevail on its claim that Defendants have engaged in violations of the foregoing law by:

a. intentionally accessing and sending malicious software, code, and instructions to the protected computers, operating systems, and computer networks of

Microsoft and the customers of Microsoft, without authorization or exceeding authorization, in order to

i. install on those computers and computer networks malicious code and thereby gain control over those computers and computer networks in order to make them part of a botnet;

ii. attack and compromise the security of those computers and computer networks by conducting remote reconnaissance, stealing authentication credentials, monitoring the activities of users, and using other instrumentalities of theft;

iii. steal and exfiltrate information from those computers and computer networks;

b. deploying computers and Internet domains to establish a command and control infrastructure by which means Defendants conducts illegal activities, including (i) installing malicious code on computers and computer networks in order to make them part of a botnet, (ii) sending unsolicited spam e-mail to Microsoft's email services, (iii) sending unsolicited spam e-mail that falsely indicates that they are from or approved by Microsoft, (iv) delivering malicious software designed to steal financial account credentials, (v) delivering malicious "ransomware" software designed to lock access to computers and demand a ransom from victims, (vi) carrying out fraudulent schemes, (vii) monitoring the activities of users and stealing information from them, and (viii) attacking computers and networks, monitoring activities of users, and theft of information;

c. corrupting Microsoft's operating system and applications on victims' computers and networks, thereby using them to carry out the foregoing activities.

4. There is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft, Microsoft's customers, and the public. There is good cause to believe that the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court.

5. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of command and control software that is hosted at and otherwise operates through the Internet domains listed in **Appendices A** and **B** to the March

5, 2020 Temporary Restraining Order and from the destruction or concealment of other discoverable evidence of Defendants' misconduct available via those domains, including on user computers infected by Defendants, if Defendants receive advance notice of this action. Based on the evidence cited in Microsoft's TRO Application and accompanying declarations and exhibits, Microsoft is likely to be able to prove that:

a. Defendants are engaged in activities that directly violate United States law and harm Microsoft and the public, including Microsoft's customers;

b. Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests;

c. Defendants are likely to delete or to relocate the command and control software at issue in Microsoft's TRO Application and the harmful and malicious software disseminated through the Internet domains listed in **Appendices A** and **B** to the March 5, 2020 Temporary Restraining Order, thereby permitting them to continue their illegal acts; and

6. Microsoft's request for relief is not the result of any lack of diligence on Microsoft's part, but instead based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), 15 U.S.C. § 1116(a) and 28 U.S.C. § 1651(a), good cause and the interest of justice require that this Order be Granted.

7. There is good cause to believe that Defendants has engaged or will engage in illegal activity using the Internet domains identified in **Appendices A** and **B** to the March 5, 2020 Temporary Restraining Order to host the command and control software and content used to infect and compromise the computers and networks of Microsoft's customers to maintain and operate the botnet. There is good cause to believe that to immediately halt the injury caused by Defendants, the Defendants' current domain set forth in **Appendix A** to the March 5, 2020 Temporary Restraining Order must be immediately transferred to the control of Microsoft and redirected to the Microsoft-secured name-servers named NS080A.microsoftinternetsafety.net and NS080B.microsoftinternetsafety.net, thus making it inaccessible to Defendants for

command and control purposes. There is good cause to believe that to immediately halt the injury caused by Defendants, each of the Defendants' prospective domains set forth in **Appendix B** to the March 5, 2020 Temporary Restraining Order must be prevented from being registered by Defendants and prevented from entering the zone file, thus making them inaccessible to Defendants for command and control purposes.

8. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants must be prohibited from accessing Microsoft's services without authorization and prohibited from sending malicious code, content and commands using the Internet domains identified in **Appendices A** and **B** to the March 5, 2020 Temporary Restraining Order to the computers of Microsoft's customers.

9. There is good cause to direct that third-party Internet registrars reasonably assist in the implementation of the Order and refrain from frustrating the implementation and purposes of this Order, pursuant to 28 U.S.C. § 1651(a) (the All Writs Act).

10. There is good cause to believe that Defendants have specifically directed their activities to computers of Microsoft's customers located in New York and the Eastern District of New York, have engaged in illegal activity using the Internet domains identified in **Appendices A** and **B** to the March 5, 2020 Temporary Restraining Order by using those domains to carry out the illegal conduct described in this Order, and to injure Microsoft, Microsoft's customers and the public. There is good cause to believe that Defendants have directed malicious code and content through the domains and the domain registration facilities of the domain registries identified in **Appendices A** and **B** to the March 5, 2020 Temporary Restraining Order.

11. There is good cause to permit notice of the instant Order and service of the

Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service, when taken in combination, are authorized by law, satisfy Due Process, satisfy Fed. R. Civ. P. 4(f)(3) and are reasonably calculated to notify Defendants of the instant Order and of this action: (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to Defendants' domain registrars and hosting companies and as agreed to by Defendants in Defendants' domain registration and/or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the U.S.; and (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent Defendants provided accurate contact information in foreign countries that are signatories to such treaties.

PRELIMINARY INJUNCTION

IT IS THEREFORE ORDERED as follows

A. Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants, are temporarily restrained and enjoined from: (1) intentionally accessing and sending malicious software or code to Microsoft and the protected computers and operating systems of Microsoft and Microsoft's customers, without or in excess of authorization, in order to infect those computers and make them part of the botnet; (2) sending malicious software to configure, deploy and operate a botnet, (3) sending unsolicited spam e-mail to Microsoft's email services, (4) sending unsolicited spam e-mail that falsely indicates that they are from or approved by Microsoft, (5) attacking and compromising the security of the computers and networks of Microsoft and its customers, (6) stealing and exfiltrating information

from computers and computer networks, (7) delivering malicious software designed to steal financial account credentials, (8) delivering malicious "ransomware" software designed to lock access to computers and demand a ransom from victims, (9) carrying out fraudulent schemes, (10) monitoring the activities of Microsoft's customers and stealing information from them, (11) attacking computers and networks, monitoring activities of users, and theft of information, (12) corrupting Microsoft's operating system and applications on victims' computers and networks, thereby using them to carry out the foregoing activities, (13) misappropriating that which rightfully belongs to Microsoft, its customers or in which Microsoft or its customers have a proprietary interest, (14) configuring, deploying, operating, or otherwise participating in or facilitating a command and control infrastructure described in the TRO Application, including but not limited to the command and control software hosted at and operating through the Internet domains set forth in **Appendices A** and **B** to the March 5, 2020 Temporary Restraining Order and through any other component or element of the command and control infrastructure at any location, and (15) undertaking any similar activity that inflicts harm on Microsoft, Microsoft's customers, or the public.

B. Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants are temporarily restrained and enjoined from (1) using and infringing Microsoft's trademarks, including specifically Microsoft's registered trademarks "Microsoft," bearing registration number 5449084, "Windows," bearing registration number 2463526, and/or other trademarks, trade names, service marks, or Internet Domain addresses or names containing or infringing such trademarks, trade names or service marks; (2) using in connection with Defendants' activities, products, or services any false or deceptive designation, representation or description of Defendants' or of their activities, whether by symbols, words,

designs or statements, which would damage or injure Microsoft or give Defendants an unfair competitive advantage or result in deception of consumers; or (3) acting in any other manner which suggests in any way that Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Microsoft, or passing off Defendants' activities, products or services as Microsoft's.

IT IS FURTHER ORDERED that the domain set forth in **Appendix A** to the March 5, 2020 Temporary Restraining Order shall be maintained by Microsoft in its account at the domain registrar MarkMonitor. The purpose of this paragraph is to ensure that Microsoft has control over the hosting and administration of the domain in its registrar account at MarkMonitor or such other registrar specific by Microsoft. Microsoft shall provide to the domain registry or registrar of record any requested registrar information or account details necessary to effectuate the foregoing.

IT IS FURTHER ORDERED that, with respect to the discrete set of dynamically generated domains set forth at **Appendix B** to the March 5, 2020 Temporary Restraining Order, that are being generated and will be generated by the botnet code for a period of 25 months from the date of this order, pursuant to stipulation and pursuant to the All Writs Act (28 U.S.C. § 1651), the domain registries shall take the following actions:

A. The domain registry and service provider Neustar, Inc., Afilias USA, Inc., Public Interest Registry and ICM Registry LLC, identified in **Appendix B** to the March 5, 2020 Temporary Restraining Order, shall take reasonable steps to prevent such domains from entering the zone file, consistent with its operational capabilities in order to prevent the domains from being controlled by the Defendants or third parties. Means of compliance with this term include, but are not limited to, implementation of proprietary systems by Neustar, Inc., Afilias USA, Inc.,

Public Interest Registry and ICM Registry LLC that automatically prevent registration of domains, or pre-registering such domains in an Afilias USA, Inc. "house account" or other means reasonably calculated to prevent registration of the dynamically generated domains by Defendants or any third party. "Dynamically generated domains" shall mean the discrete list of domains automatically generated by the botnet software running on test machines in a laboratory environment and which is not subject to discretion. Nothing in the foregoing shall prevent registration or activation of the domains by Microsoft or its security industry partners Stichting Registrar of Last Resort Foundation and The Shadowserver Foundation for purposes of analysis of the botnet.

B. The domain registry and service provider Verisign, Inc., identified in **Appendix B** to the March 5, 2020 Temporary Restraining Order, shall take reasonable measures, at the registry's discretion, to cause the dynamically generated domains in **Appendix B** to the March 5, 2020 Temporary Restraining Order to be unresolvable. "Dynamically generated domains" shall mean the discrete list of domains automatically generated by the botnet software running on test machines in a laboratory environment and which is not subject to discretion. Nothing in the foregoing shall prevent registration or activation of the domains by Microsoft or its security industry partners Stichting Registrar of Last Resort Foundation and The Shadowserver Foundation for purposes of analysis of the botnet.

C. The foregoing domain registries shall treat any domain names set forth in **Appendix B** the March 5, 2020 Temporary Restraining Order that have been registered as if they are included in **Appendix A** to that order, unless otherwise instructed by Microsoft or its delegates.

IT IS FURTHER ORDERED that copies of this Order, the Complaint and all other

pleadings filed in this action may be served upon the Defendants by any means authorized by law, including the combination of: (1) transmission by email, facsimile, mail and/or personal delivery 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, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the U.S.; and (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent Defendants provided accurate contact information in foreign countries that are signatories to such treaties.

IT IS SO ORDERED

Entered this 2nd day of April, 2020

s/LDH

LaSHANN DeARCY HALL
United States District Judge