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

MICROSOFT CORPORATION, a Washington corporation, and FS-ISAC, INC., a Delaware corporation, Plaintiffs, v. JOHN DOES 1-2, CONTROLLING A COMPUTER BOTNET AND THEREBY INJURING PLAINTIFFS, AND THEIR CUSTOMERS AND MEMBERS, Defendants.	Civil Action No: 1:20cv1171 **FILED UNDER SEAL**

***EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

Plaintiffs Microsoft Corp. ("Microsoft") and Financial Services – Information Sharing And Analysis Center, Inc. ("FS-ISAC") (collectively "Plaintiffs") have filed a complaint for injunctive and other relief pursuant to: (1) the Copyright Act (17 U.S.C. § 101, *et seq.*); (2) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (3) the Electronic Communications Privacy Act (18 U.S.C. § 2701); (4) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); and (5) the common law of trespass, unjust enrichment and conversion. Plaintiffs have 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).

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Plaintiffs' Application for an Emergency Temporary Restraining Order, 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 1-2 ("Defendants") under the Copyright Act (17 U.S.C. §§ 106 and 501 *et seq.*), the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125) and the common law of trespass to chattels, unjust enrichment and conversion.

2. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Copyright Act (17 U.S.C. §§ 106 and 501 *et seq.*), the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125) and constitute trespass to chattels, unjust enrichment and conversion, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. Microsoft owns the registered copyrights in the Windows 8 Software Development Kit ("SDK"), Reg. No. TX 8-888-365 ("Copyrighted Work"). Microsoft's Copyrighted Work is an original, creative work and copyrightable subject matter under the laws of the United States. *See* 17 U.S.C. § 102(a); *see also Oracle America, Inc. v. Google Inc.*, 750 F.3d 1339 (Fed. Cir. 2014) (holding the structure, sequence, and organization of declaring computer code qualifies as an original work under the Copyright Act).

4. Microsoft owns the registered trademarks "Microsoft" and "Windows" used in connection with its services, software and products. FS-ISAC's member organizations have invested in developing their brands, trademarks, and trade names in association with the financial services they offer.

5. 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 Plaintiffs' Brief in Support of Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Application"),

and the accompanying declarations and exhibits, demonstrates that Plaintiffs are likely to prevail on their claims that Defendants have engaged in violations of the foregoing law by:

a. directly, contributorily and through inducement, infringing Microsoft's Copyrighted Work by reproducing, distributing, and creating derivative works in their malicious software, which includes code that is literally copied from, substantially similar to and derived from the Copyrighted Work, in violation of Microsoft's exclusive rights at least under 17 U.S.C. § 101 *et seq.* without any authorization or other permission from Microsoft;

b. transmitting malicious code containing the Copyrighted Work through Internet Protocol addresses ("IP Addresses") to configure, deploy and operate a botnet;

c. intentionally accessing and sending malicious software, code, and instructions to the protected computers and operating systems of the customers or associated member organizations of Microsoft and FS-ISAC, without authorization and 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 the computer botnet known as the "Trickbot" botnet (the "botnet");

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

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

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

e. creating false websites that falsely indicate that they are associated with or approved by Plaintiffs or Plaintiffs' member organizations;

f. stealing personal and financial account information from computer users; and

g. using stolen information to steal money from the financial accounts of those users.

6. There is good cause to believe that if such conduct continues, irreparable harm will occur to Plaintiffs, Plaintiffs' customers and member organizations, 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;

7. 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 botnet command and control software that is hosted at and otherwise operates through the IP addresses listed in **Appendix A** and from the destruction or concealment of other discoverable evidence of Defendants' misconduct available at those locations if Defendants receive advance notice of this action. Based on the evidence cited in Plaintiffs' TRO Application and accompanying declarations and exhibits, Plaintiffs are likely to be able to prove that:

a. Defendants are engaged in activities that directly violate United States law and harm Plaintiffs and the public, including Plaintiffs' customers and member-organizations;

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 botnet command and control software at issue in Plaintiffs' TRO Application and the harmful and malicious software, infringing Microsoft's Copyrighted Work and trademarks, disseminated through the IP Addresses listed in **Appendix A** to this Order, thereby permitting them to continue their illegal acts; and

d. Defendants are likely to warn their associates engaged in such activities if informed of Plaintiffs' action.

8. Plaintiffs' request for this emergency *ex parte* relief is not the result of any lack of diligence on Plaintiffs' 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 without prior notice to Defendants, and accordingly, Plaintiffs are relieved of the duty to provide Defendants with prior notice of Plaintiffs' motion.

9. There is good cause to believe that Defendants have specifically directed their activities to computers of Plaintiffs' customers and member organizations located in the Eastern District of Virginia, have engaged in illegal activity using the IP Addresses identified in **Appendix A** to this Order that are registered to command and control servers located at data

centers and/or hosting companies set forth in **Appendix A**, to direct malicious botnet code and content through the Internet to said computers of Plaintiffs' customers and member organizations to further perpetrate their fraud on Plaintiffs' customers and member organizations.

10. There is good cause to believe that Defendants have engaged in illegal activity using the data centers and/or Internet hosting providers identified in **Appendix A** to host command and control software and the malicious botnet code and content used to maintain and operate the botnet at computers, servers, electronic data storage devices, or media at the IP Addresses listed in **Appendix A**.

11. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants' IP Addresses identified in **Appendix A** must be immediately disabled; Defendants' computer resources related to such IP Addresses must be disconnected from the Internet; Defendants must be prohibited from accessing Defendants' computer resources related to such IP Addresses; and to prevent the destruction of data and evidence located on those computing resources.

12. There is good cause to believe that in order to immediately halt the injury caused by Defendants and to ensure the future prosecution of this case it not rendered fruitless by attempts to delete, hide, conceal, or otherwise render inaccessible the software components that create, distribute, and are involved in the creation, perpetuation, and maintenance of the botnet and prevent the unauthorized copying, reproduction, distribution, public display, and creation of derivative works in Microsoft's Copyrighted Work and prevent the creation and distribution of unauthorized copies of the registered trademarks of Microsoft and FS-ISAC's member organizations and carry out other harmful conduct, with respect to the Defendants' most current, active command and control servers hosted at the IP Addresses, the following actions should be taken. The data centers and/or hosting companies set forth in **Appendix A** should take reasonable steps to block incoming and/or outgoing traffic on their respective networks that originates or has been sent from and/or to the IP Addresses identified in **Appendix A**, such that

said traffic will not reach victim end-user computers on the ISPs' respective networks and/or the computers at the IP Addresses in **Appendix A**, and should take other reasonable steps to block such traffic to and/or from any other IP addresses to which Defendants may move the botnet infrastructure, identified by Plaintiffs and which the Court may order to be subject to this Order, to ensure that Defendants cannot use such infrastructure to control the botnet.

13. There is good cause to believe that Defendants may change the IP Addresses that they use to conduct illegal activities, and that Plaintiffs may identify and update the IP Addresses listed in **Appendix A** to this Order as may be reasonably necessary to account for additional IP Addresses associated with Defendants just prior to the execution of this Order and within a reasonable time thereafter should Defendants attempt to evade and defy this Order.

14. There is good cause to permit notice of the instant Order, notice of the Preliminary Injunction hearing 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 are authorized by law, satisfy Due Process, and satisfy Fed. R. Civ. P. 4(f)(3) and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to Defendants' data centers and/or hosting companies and as agreed to by Defendants in Defendants' data center 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.

15. There is good cause to believe that the harm to Microsoft and FS-ISAC's member organizations of denying the relief requested in the TRO Application outweighs any harm to any legitimate interests of Defendants and that there is no undue burden to any third party.

TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

IT IS THEREFORE ORDERED that, Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from: (1) intentionally accessing and sending malicious software or code to Plaintiffs and the protected computers and operating systems of Plaintiffs' customers and associated member organizations, without authorization, in order to infect those computers and make them part of any botnet, (2) sending malicious code to configure, deploy and operate a botnet, (3) attacking and compromising the security of the computers and networks of Plaintiffs, their customers, and any associated member organizations, (4) stealing and exfiltrating information from computers and computer networks, (5) creating false websites that falsely indicated that they are associated with or approved by Plaintiffs or Plaintiffs' member organizations; (6) configuring, deploying, operating, or otherwise participating in or facilitating the botnet described in the TRO Application, including but not limited to the command and control software hosted at and operating through the IP Addresses set forth herein and through any other component or element of the botnet in any location; (7) delivering malicious software designed to steal financial account credentials, (8) monitoring the activities of Plaintiffs, Plaintiffs' customers or member associations and stealing information from them, (9) attacking computers and networks, monitoring activities of users, and theft of information, (10) corrupting Microsoft's operating system and applications on victims' computers and networks, thereby using them to carry out the foregoing activities, (11) misappropriating that which rightfully belongs to Plaintiffs, Plaintiffs' customers or member associations or in which Plaintiffs have a proprietary interests, and (12) undertaking any similar activity that inflicts harm on Plaintiffs, Plaintiffs' customers or member associations, or the public.

IT IS FURTHER ORDERED that, Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from: (1) reproducing, distributing, creating derivative works, and/or otherwise infringing Microsoft's

Copyrighted Work, bearing registration number TX 8-888-365; (2) using and infringing Microsoft's trademarks, including specifically Microsoft's registered trademarks "Microsoft," "Windows," "Outlook" and "Word" logo bearing registration numbers 2872708, 5449084, 2463526, 4255129 and 77886830; and/or the trademarks of financial institution members of FS-ISAC; (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 Plaintiffs or their member organizations 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 Plaintiffs' or their member organizations.

IT IS FURTHER ORDERED that, with respect to any of the IP Addresses set forth in **Appendix A** to this Order, the data centers and/or hosting providers identified in **Appendix A** to this Order shall take reasonable best efforts to implement the following actions:

A. Take reasonable steps to identify incoming and/or outgoing Internet traffic on their respective networks that originates and/or is being sent from and/or to the IP Addresses identified in **Appendix A**;

B. Take reasonable steps to block incoming and/or outgoing Internet traffic on their respective networks that originate and/or are being sent from and/or to the IP Addresses identified in **Appendix A**, by Defendants or Defendants' representatives or resellers, except as explicitly provided for in this Order;

C. Take other reasonable steps to block such traffic to and/or from any other IP addresses or domains to which Defendants may move the botnet infrastructure, identified by Microsoft in a supplemental request to this Order, to ensure that Defendants cannot use such infrastructure to control the botnet.

D. Completely disable the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with the IP Addresses set forth in **Appendix A** and make them inaccessible from any other computer on the Internet, any internal network, or in any other manner, to Defendants, Defendants' representatives and all other persons, except as otherwise ordered herein;

E. Completely, and until further order of this Court, suspend all services to Defendants or Defendants' representatives or resellers associated with the IP Addresses set forth in **Appendix A**;

F. Transfer any content and software hosted at the IP Addresses listed in **Appendix A** that are not associated with Defendants, if any, to new IP Addresses not listed in **Appendix A**; notify any non-party owners of such action and the new IP addresses, and direct them to contact Microsoft's counsel, Gabriel M. Ramsey, Crowell & Moring LLP, 3 Embarcadero Ctr., 26th Floor, San Francisco, CA 94111, gramsey@crowell.com, (Tel: 415-365-7207), to facilitate any follow-on action;

G. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from publicizing this Order until this Order is executed in full, except as necessary to communicate with hosting companies, data centers, the Plaintiffs or other ISPs to execute this order;

H. Not enable, and shall take all reasonable steps to prevent, any circumvention of this order by Defendants or Defendants' representatives associated with the IP Addresses, including without limited to enabling, facilitating, and/or allowing Defendants or Defendants' representatives or resellers to rent, lease, purchase, or otherwise obtain another IP Address associated with your services;

I. Preserve, retain and produce to Plaintiffs all documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling the IP Addresses set forth in **Appendix A**, including any and all individual or entity names, mailing

addresses, e-mail addresses, facsimile numbers and telephone numbers or similar contact information, including but not limited to such contact information reflected in billing, usage, access and contact records and all records, documents and logs associated with Defendants' or Defendants' Representatives' use of or access to the IP Addresses;

J. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order; and

K. Completely preserve the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with the IP Addresses set forth in **Appendix A**, and preserve all evidence of any kind related to the content, data, software or accounts associated with such IP addresses and such computer hardware, such that such evidence of Defendants' unlawful activities is preserved.

IT IS FURTHER ORDERED that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means authorized by law, including any one or combination of (1) personal delivery upon Defendants who provided accurate contact information in the U.S., if any; (2) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided accurate contact information in foreign countries that are signatory to such treaties, if any, (3) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their hosting companies and as agreed to by Defendants in their hosting agreements, (4) publishing notice on a publicly available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

IT IS FURTHER ORDERED, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before this Court on October 20th, 2020, at 2:00 p.m. to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against the Defendants, enjoining them from the conduct temporarily restrained by the preceding provisions of this Order.

IT IS FURTHER ORDERED that Microsoft shall post bond in the amount of $75,000 as cash to be paid into the Court registry.

IT IS FURTHER ORDERED that Plaintiffs may identify and update the IP addresses to this Order as may be reasonably necessary to account for additional IP addresses associated with the Trickbot Botnet just prior to the execution of this Order.

IT IS FURTHER ORDERED that the Defendants shall file with the Court and serve on Plaintiffs' counsel any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later than two (2) days prior to the hearing on Microsoft's request for a preliminary injunction. Plaintiffs may file responsive or supplemental pleadings, materials, affidavits, or memoranda with the Court and serve the same on counsel for the Defendants no later than one (1) day prior to the preliminary injunction hearing in this matter. Provided that service shall be performed by personal or overnight delivery, facsimile or electronic mail, and documents shall be delivered so that they shall be received by the other parties no later than 4:00 p.m. (Eastern Standard Time) on the appropriate dates listed in this paragraph.

IT IS SO ORDERED

Entered this 6th day of October, 2020.

/s/
Anthony J. Trenga
United States District Judge

APPENDIX A

APPENDIX A

LIST OF IP ADDRESSES AND HOSTING COMPANIES ASSOCIATED WITH TRICKBOT'S COMMAND AND CONTROL SERVERS

IP Addresses of Command and Control Servers	Hosting Companies/Data Centers Where Defendants Have Placed the Command and Control Servers,
104.161.32.103 104.161.32.105 104.161.32.106 104.161.32.109 104.161.32.118	Input Output Flood, LLC d/b/a Ioflood 9030 W. Sahara Ave., Suite 703 Las Vegas, NV 89117 Input Output Flood, LLC d/b/a Ioflood c/o Phoenix NAP, LLC d/b/a phoenixNAP 3402 E University Dr. #6 Phoenix, AZ 85034
104.193.252.221	Hosting Solution Ltd. c/o Hurricane Electric LLC 48233 Warm Springs Blvd Fremont, CA 94539 Hurricane Electric LLC 760 Mission Ct. Fremont, CA 94539
107.155.137.19 107.155.137.28 107.155.137.7 162.216.0.163 23.239.84.132 23.239.84.136	Nodes Direct Holdings, LLC 1650 Margaret St Suite 302-351 Jacksonville, FL 32204 Nodes Direct Holdings, LLC 4495 Roosevelt Blvd, Suite 304-241 Jacksonville, FL 32210 Nodes Direct Holdings LLC c/o Cologix, Inc. 421 W. Church St., Suite 429 Jacksonville, FL 32202
107.174.192.162 107.175.184.201	Virtual Machine Solutions LLC 1600 Sawtelle Blvd., Suite 308 Los Angeles, CA 90025

	Virtual Machine Solutions LLC 2801 Robin Rd. Midwest City. OK 73110 Virtual Machine Solutions LLC c/o Velocity Servers, Inc. d/b/a ColoCrossing 325 Delaware Ave., Suite 300 Buffalo, NY 14202 Velocity Severs, Inc. d/b/a ColoCrossing 8185 Sheridan Dr Buffalo, NY 14221-6002
139.60.163.45	Hostkey USA, Inc. c/o Smyle & Associates 122 East 42nd St., Suite 3900 New York NY 10168 Hostkey USA, Inc. c/o Webair Internet Development Company Inc. 501 Franklin Avenue, Suite 200 Garden City, NY 11530 Hostkey USA, Inc. c/o Webair Internet Development Company Inc. 1025 Old Country Road Westbury, NY 11590 Hostkey USA, Inc. c/o Hurricane Electric LLC 501 Franklin Avenue, Suite 200 Garden City, NY 11530 Hurricane Electric LLC 760 Mission Ct. Fremont, CA 94539
156.96.46.27	Fastlink Network, Inc. 624. S. Grand Ave. Los Angeles, CA 90017 Fastlink Network, Inc. Fastlink Network – Newtrend Division P.O. Box 17295

	Encino, CA 91416 Fastlink Network, Inc. c/o Incorp Services, Inc. 5716 Corsa Ave, Suite 110 Westlake Village, CA 91362 Fastlink Network, Inc. 624. S. Grand Ave. Los Angeles, CA 90017 Fastlink Network, Inc. and VolumeDrive, Inc. 1143 Northern Blvd. Clarks Summit PA 18411 Fastlink Network, Inc. and VolumeDrive, Inc. 9 East Market St Wilkes Barre, PA 18701
195.123.241.13 195.123.241.55	Green Floid LLC c/o Business Filings Inc. 1200 South Pine Island Road Plantation, FL 33324 Green Floid LLC 119 Grimsby St. – Staten Island New York, NY 10306 Green Floid LLC 2707 East Jefferson Street Orlando, FL, 32803 Green Floid LLC ITL-Bulgaria Ltd. c/o Equinix, Inc. 1920 E. Maple Ave. El Segundo, CA 90245 Equinix, Inc. One Lagoon Dr. Redwood City, CA 94065

	Equinix, Inc. c/o United Agent Group, Inc. 4640 Admiralty Way, 5th Floor Marina del Rey, CA 90292
162.247.155.165	Twinservers Hosting Solutions Inc. 23 Meadowview Circle Nashua, NH 03062 Twinservers Hosting Solutions, Inc. c/o DataSite Atlanta BPC, LLC c/o Burges Property & Co. 1130 Powers Ferry Pl. Marietta, GA 30067 DataSite Atlanta BPC, LLC Burges Property & Co. 2658 Del Mar Heights Rd. #558 Del Mar, CA, 92014 Twinservers Hosting Solutions, Inc. c/o Performive LLC 1130 Powers Ferry Pl. Marietta, GA 30067 Performive LLC c/o Holt Ney Zatcoff & Wasserman, LLP 100 Galleria Parkway, Suite 1800 Atlanta, GA, 30339