

**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  
THEREBY INJURING PLAINTIFFS  
AND ITS CUSTOMERS,

Defendants.

Civil Action No: 1:19-cv-01582 (LO/JFA)

**PRELIMINARY INJUNCTION ORDER**

Plaintiff Microsoft Corp. (“Microsoft”) has filed a complaint for injunctive and other relief pursuant to: 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) the Electronic Communications Privacy Act (18 U.S.C. § 2701); (3) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); (4) the Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)); and (5) the common law of trespass to chattels, unjust enrichment, conversion and intentional interference with contractual relationships. 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 December 18, 2019, the Court issued a temporary restraining order and order to show cause why an injunction

should not issue. 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, memorandum, and all other pleadings and papers relevant to Microsoft's request for a Preliminary Injunction, 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 Doe 1 and 2 ("Defendants") under 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), the Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)), and the common law of trespass to chattels, unjust enrichment, conversion, and intentional interference with contractual relationships.

2. Defendants have not responded to the Court's December 18, 2019 Order to Show Cause.

3. 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), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)) 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.

4. Microsoft owns the registered trademarks Microsoft, Windows, Hotmail, Outlook, and Office 365 and numerous other trademarks used in connection with its services, software

and products.

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 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. steal and exfiltrate information from those computers and computer networks;
  - ii. infect those computers and computer networks with malicious code and thereby gain control over those computers and computer networks;
  - iii. 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;
- b. deploying computers and Internet domains to establish a command and control infrastructure by which means Defendants conduct illegal activities, including attacks on 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 monitor the activities of users and steal information from them;

6. 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 enjoined 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 the Internet domains listed in Appendix A to the Complaint and also attached to this Order ("Appendix A") and from the destruction or concealment of other discoverable evidence of Defendants' misconduct available via those domains. 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; and
- c. Defendants are likely to continue the harmful acts set forth in Microsoft's TRO Application through the Internet domains listed in Appendix A, absent continued relief.

8. Microsoft's request for this preliminary injunction 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;

9. There is good cause to believe that Defendants have specifically directed their activities to computers of Microsoft's customers located in the Eastern District of Virginia, have engaged in illegal activity using the Internet domains identified in Appendix A by directing malicious code and content to said computers of Microsoft's customers, to further perpetrate their illegal conduct victimizing Microsoft's customers. There is good cause to believe that Defendants have directed said malicious code and content through certain instrumentalities – specifically the domains and the domain registration facilities of the domain registries identified

in Appendix A.

10. There is good cause to believe that Defendants have engaged in illegal activity by using the domain registration facilities of the domain registries identified in Appendix A to register the Internet domains identified in Appendix A, so as to deliver from those domains the malicious code, content, and commands that Defendants use to access Microsoft's services without authorization and to infect and compromise the computers of Microsoft's customers, and to receive the information stolen from those computers.

11. There is good cause to believe that Defendants have engaged in illegal activity by using deceptive and fake methods to steal computer users' login and/or account credentials and to use such credentials for illegal purposes.

12. There is good cause to believe that to halt the injury caused by Defendants, Defendants must continue to be prohibited from accessing Microsoft's services without authorization and prohibited from sending malicious code, content and commands from the Internet domains identified in Appendix A to the computers of Microsoft's customers.

13. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains identified in Appendix A to deliver command and control software and content used to infect and compromise the computers and networks of Microsoft's customers and to steal information from them. There is good cause to believe that to halt the injury caused by Defendants, each of Defendants' current and prospective domains set forth in Appendix A shall continue to be maintained within the control of Microsoft at the registrar account set forth in the Temporary Restraining Order, thus making them inaccessible to Defendants for command and control purposes.

14. There is good cause to believe that Defendants may change or put into place new

Internet domains that they use to conduct illegal activities, and that Microsoft may identify and move the Court to update the domains listed in Appendix A as may be reasonably necessary to account for additional Internet domains associated with Defendants should Defendants attempt to evade and defy this Order.

15. There is good cause to permit notice of the instant Order and service of all other pleadings 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: (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.; or (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 signatory to such treaties.

**PRELIMINARY INJUNCTION**

**IT IS THEREFORE ORDERED** that, Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants, are 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 authorization, in order to infect those computers; (2) intentionally attacking and compromising computers or computer networks of Microsoft or Microsoft's customers, to monitor the activities

of the owners or users of those computers or computer networks, and to steal information from those computers or networks; (3) 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 Appendix A and through any other component or element of the command and control infrastructure at any location; (4) stealing information from Microsoft's customers; (5) misappropriating that which rightfully belongs to Microsoft, its customers, or in which Microsoft or its customers have a proprietary interest; (6) downloading or offering to download additional malicious software onto the computers of Microsoft's customers; or (7) undertaking any similar activity that inflicts harm on Microsoft, Microsoft's customers, or the public.

**IT IS FURTHER ORDERED** that, Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants are enjoined from (1) using and infringing Microsoft's trademarks, including specifically Microsoft's registered trademarks "Microsoft," "Windows," "Hotmail," "Outlook," and "Office 365," and/or other trademarks, trade names, service marks, or Internet Domain addresses or names, or any confusingly similar variant; (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.

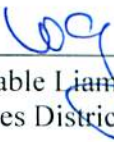
**IT IS FURTHER ORDERED** that the domains set forth in Appendix A to the

Complaint and Appendix A to this 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 specified 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 copies of this Order and all other pleadings and documents in this action may be served by any means authorized by law, including (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.; or (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 signatory to such treaties.

**IT IS SO ORDERED**

Entered this 3<sup>rd</sup> day of January, 2020

  
\_\_\_\_\_  
The Honorable Liam O'Grady  
United States District Judge