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: 1:21-cv-822 (RDA/IDD)

[PROPOSED] DEFAULT JUDGMENT AND ORDER FOR PERMANENT INJUNCTION

This matter came before the Court on Plaintiff Microsoft Corporation's ("Microsoft") Motion for Default Judgment and Permanent Injunction. Plaintiff has established the elements of their claims pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030), (2) the Stored Communications Act (18 U.S.C. § 2701 *et seq*.), (3) the Virginia Computer Crimes Act (Virginia Code Ann. § 18.2-152.5:1), and (4) the common law of trespass to chattels and conversion. Defendants have failed to appear, plead, or otherwise defend this action. Plaintiff is entitled to default judgment under Rule 55(b) of the Federal Rules of Civil Procedure and a permanent injunction pursuant to Rule 65 of the Federal Rules of Civil Procedure, and 28 U.S.C. § 1651(a) (the All-Writs Act):

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, memorandum, and all other pleadings and papers relevant to Plaintiff's Motion for Default Judgment and Entry of a Permanent Injunction, the Court hereby makes the following findings of fact and conclusions of law:

1. The Defendants were properly served with Plaintiff's summons, complaint, and other pleadings in this action and were provided with adequate notice of this action through means authorized by law, satisfying Due Process, satisfying Fed. R. Civ. P. 4 and reasonably calculated to provide Defendants with notice. Specifically, Defendants have been served via e-mail at e-mail addresses associated with infrastructure used by Defendants to carry out the activity that is the subject of the complaint and by publication on the public website http://www.noticeofpleadings.com/maliciousdomains.

2. Defendants failed to appear, plead, or otherwise defend against the action.

3. The time for responding to Plaintiff's complaint was 21 days from service of the summons and complaint, and more than 21 days have elapsed since Plaintiff effected service. The Clerk properly entered default pursuant to Rule 55(a) on February 24, 2022. Dkt. No. 35.

4. This Court has jurisdiction over the subject matter of the case and venue is proper in this judicial district.

5. Plaintiff has established a case for personal jurisdiction over Defendants under Rules 4(k)(1) and 4(k)(2) of the Federal Rules of Civil Procedure. Defendants have purposefully availed themselves of the privilege of conducting malicious conduct—including violations under the Computer Fraud and Abuse Act and the Stored Communications Act—in the United States in general, and in Virginia in particular.

6. Plaintiff is entitled to entry of judgment and a permanent injunction against Defendants.

7. The evidence of record indicates that no Defendant is an infant or incompetent.

8. 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 Stored Communications Act

(18 U.S.C. § 2701 *et seq*.), the Virginia Computer Crimes Act (Virginia Code Ann. § 18.2-152.5:1), the common law of trespass to chattels and conversion.

9. Microsoft owns the registered trademarks "Microsoft" and "Windows" used in connection with its services, software and products.

10. After receiving notice of the Preliminary Injunction, the Defendants have continued to engage in the conduct enjoined by the Preliminary Injunction, and therefore continue to violate the Preliminary Injunction. In particular, Defendants have continued:

a. targeting Microsoft's O365 customers and services and conduct malicious activity including business email compromise attacks, in order to:

   i. use stolen O365 login credentials and gain access to Microsoft customers' O365 accounts;

   ii. monitor the compromised account, emails, and contact list to identify opportunities to target the compromised O365 customer's contacts for financial fraud, which may also include forwarding emails with key financial words like "invoice," "accounts receivable," "funds," "overdue," "payroll," or "IBAN," and masking their activities to evade detection;

   iii. use stolen credentials to gain unauthorized access to Office 365 accounts and having monitored account activity, identify additional victims either in the compromised O365 customer's business or their wider network;

   iv. register homoglyph domains to impersonate legitimate businesses (hereinafter, "homoglyph imposter domains"), host these homoglyph imposter domains on a fraudulently procured O365 tenant, establish spoof email addresses impersonating one or more of the foregoing parties to deceive such parties into sending wire payments to Defendants;

b. intentionally access and send malicious software, code, and instructions to the protected computers and operating systems of Microsoft customers without authorization and exceeding authorization;

c. attacking and compromising 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;

d. stealing and exfiltrating information from those computers and computer networks;

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

f. creating false websites that falsely indicate that they are associated with or approved by Plaintiff;

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

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

11. There is good cause to believe that Defendants are likely to continue the foregoing conduct and to engage in the illegal conduct and purposes enjoined by the Preliminary Injunction and this Permanent Injunction, unless Defendants are permanently restrained and enjoined and unless final relief is ordered to expeditiously prevent Defendants from impersonating legitimate businesses by registering homoglyph imposter domains for such prohibited and unlawful purposes, on an ongoing basis.

12. There is good cause to believe that, unless Defendants are permanently restrained and enjoined and unless further relief is ordered to expeditiously prevent Defendants from maintaining the registration of new homoglyph domains for purposes enjoined by the Preliminary Injunction and this Permanent Injunction, on an ongoing basis, immediate and irreparable harm will result to Plaintiff, Plaintiff's customers and to the public, from the Defendants' ongoing violations.

13. There is good cause to believe that to halt the injury caused by Defendants, they must be prohibited from using homoglyph domain names, as set forth in **Appendix A** to the default judgment and permanent injunction, and Defendants must be prohibited from accessing Defendants' computer resources related to such domain names.

14. The hardship to Plaintiff and their customers that will result if a permanent injunction does not issue weighs in favor of an injunction. Defendants will suffer no cognizable

injury as a result of being enjoined from further illegal conduct.

15. There is good cause to permit notice of the instant Order, further orders of the court and service of the Complaint by formal and alternative means. 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 their hosting companies, and (2) publishing notice on the publicly available website http://www.noticeofpleadings.com/maliciousdomains.

FINAL JUDGMENT AND PERMANENT INJUNCTION

IT IS THEREFORE ORDERED that in accordance with Fed. R. Civ. P. 65(b) and 15 U.S.C. § 1116(a) and 28 U.S.C. § 1651(a) and the court's inherent equitable authority, good cause and the interests of justice, Plaintiff's Motion for Default Judgment and Entry of a Permanent Injunction is Granted.

IT IS FURTHER ORDERED that Defendants are in default, and that judgment is awarded in favor of Plaintiff and against Defendants.

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) intentionally accessing and sending malicious software or code to Plaintiff and the protected computers and operating systems of Plaintiff's customers, without authorization, in order to infect those computers and make them part of any malicious command and control infrastructure, (2) sending malicious code to configure, deploy and operate a malicious infrastructure, (3) attacking and compromising the security of the computers and networks of Plaintiff and their customers, (4) stealing and exfiltrating information from computers and computer networks, (5)

creating false websites that deceptively indicated that they are associated with or approved by Plaintiff; (6) configuring, deploying, operating, or otherwise participating in or facilitating the malicious infrastructure described in the TRO Application, including but not limited to creating homoglyph imposter domains; (7) stealing credentials through among other means including sending credential phishing emails, (8) monitoring the activities of Plaintiff and its customers 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 Plaintiff and Plaintiff's customers, and (12) undertaking any similar activity that inflicts harm on Plaintiff, Plaintiff's customers, 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) 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; (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 Plaintiff 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 Plaintiff, or passing off Defendants' activities, products or services as Plaintiff's.

IT IS FURTHER ORDERED that Defendants must be enjoined from using domain names identified at **Appendix A** used to carry out the activities enjoined herein and Defendants must be prohibited from accessing Defendants' computer resources related to such domain names.

IT IS FURTHER ORDERED that copies of this Order and all other pleadings and documents in this action, including orders and determinations, 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 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/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 ____ day of _____, 2022

_____
Rossie D. Alston, Jr.
United States District Judge

CERTIFICATE OF SERVICE

I hereby certify that on March 9, 2022, I will electronically file the foregoing with the Clerk of Court using the CM/ECF system.

Copies of the forgoing were also served on the defendants listed below by electronic mail:

John Does 1-2:
sam@enertrak.co
vpickrell@lindsayprecast.co
thamric@lindsayprecast.co
dwolosiansky@lindsayprecast.co
asaxon@martellotech.co
felorado79@gmail.com
angernrpraving@gmail.com
marksincomb26@gmail.com
clint1566@gmail.com
resultlogg44@gmail.com
zohoferdz1@gmail.com
mbakudgorilla@yahoo.com

Respectfully submitted,

/s/ David J. Ervin

David J. Ervin (VA Bar No. 34719)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Telephone: (202) 624-2500
Fax: (202) 628-5116
dervin@crowell.com

Attorney for Plaintiff Microsoft Corp.