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 1-8, CONTROLLING A COMPUTER BOTNET THEREBY INJURING PLAINTIFFS, AND THEIR CUSTOMERS AND MEMBERS, Defendants.	Civil Action No: 1:14cv811 LOG/TCB

[PROPOSED] ORDER GRANTING MICROSOFT'S MOTION FOR DEFAULT JUDGMENT AND ENTRY OF A PERMANENT INJUNCTION

This matter came before the Court on Plaintiffs Microsoft Corp. ("Microsoft") and Financial Services – Information Sharing And Analysis Center, Inc. ("FS-ISAC") (collectively "Plaintiffs") Motion for Default Judgment and Entry of Preliminary Injunction. Plaintiffs have established the elements of their claims 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)); and (4) the common law of trespass, unjust enrichment and conversion. Defendants failed to appear, plead, or otherwise defend this action. Plaintiffs are entitled to default judgment under Rule 55(b) and a permanent injunction 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 a preliminary injunction, the Court hereby makes the following findings of fact and conclusions of law:

1. Defendants John Does 1-8 were properly served with Plaintiffs' 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 by publication on a the public website http://botnetlegalnotice.com/shylock/ and via e-mail at e-mail addresses associated with the malicious infrastructure underlying the Shylock botnet, both of which are means of service authorized by this Court's prior orders. E-mail is Defendants primary method of communication regarding the infrastructure underlying the Shylock botnet.

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

3. The time for responding to Plaintiffs' complaint was 21 days from service of the summons and complaint, and more than 21 days have elapsed since Plaintiffs effected service. The Clerk properly entered default pursuant to Rule 55(a) on February 3, 2015.

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

5. Plaintiffs are entitled to entry of judgment and a permanent injunction against Defendants.

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

7. 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) and constitute trespass to chattels, unjust enrichment and conversion;

8. Microsoft owns the registered trademarks Internet Explorer®, 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.

9. 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 in the record demonstrates that Defendants have engaged in violations of the foregoing law by:

a. intentionally accessing and sending malicious software 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 infect those computers and make them part of the computer botnet known as the "Shylock" botnet (the "botnet");
b. sending malicious code to configure, deploy and operate a botnet;
c. generating and sending unsolicited messages through Microsoft's Skype application and service that falsely indicate they are from or approved by Microsoft;
d. creating false websites that falsely indicate that they are associated with or approved by Plaintiffs or Plaintiffs' member organizations;
e. using deceptive telephone numbers purporting to be associated with FS-ISAC's member organizations, in order to steal computer users' credentials;
f. stealing personal and financial account information from computer users;
g. using stolen information to steal money from the financial accounts of those users; and
h. delivering malicious code.

10. 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 permanently restrained from doing so by Order of this Court;

11. 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 Internet domains identified in Appendix A to this Order by directing malicious botnet code and content to said computers of Plaintiffs' customers and member organizations; by directing malicious botnet code and content to said computers of Plaintiffs' customers and member organizations, to further perpetrate their fraud on Plaintiffs' customers and member organizations. There is good cause to believe that Defendants have directed said malicious botnet code and content through the domains identified in Appendix A.

12. There is good cause to believe that Defendants have engaged in illegal activity by using deceptive and fake telephone numbers specifically to steal computer users' login and/or financial account credentials and to use such credentials to steal funds from such users.

13. There is good cause to believe that to halt the injury caused by Defendants, Defendants must be prohibited from sending malicious botnet code and content from the Internet domains, identified in Appendix A. There is good cause to believe that to halt the injury caused by Defendants, Defendants must also be prohibited from sending or receiving telephone calls to steal computer users' credentials and continue their fraudulent conduct on Plaintiffs' customers and member organizations.

14. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains identified in Appendix A to this Order to host the command and control software and content used to maintain and operate the botnet. There is good cause to believe that to halt the injury caused by Defendants, ownership of each of Defendants' current and prospective domains set forth in Appendix A must be permanently transferred to Microsoft.

15. The hardship to Plaintiffs and their customers and members 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.

16. An injunction to prevent further illegal conduct by Defendants is in the public interest.

17. There is good cause to permit notice of the instant Order 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 domain registrars and hosting companies and as agreed to by Defendants in their domain registration and/or hosting agreements, and (2) publishing notice on a publicly available Internet website.

IT IS THEREFORE ORDERED that, Plaintiffs 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 Plaintiffs and against Defendants, and each of them.

IT IS FURTHER ORDERED that Defendants, their representatives and persons who are in active concert or participation with them are permanently 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) generating and sending unsolicited messages that falsely indicate said messages are from or approved by Microsoft or others; (4) creating false websites that falsely indicated that they are associated with or approved by Plaintiffs or Plaintiffs' member organizations; (5) 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 Internet domains, domain name servers, and IP addresses; (6) using deceptive telephone numbers purporting to be associated with Plaintiffs' member organizations in order to steal computer users' credentials; (7) stealing information, money, or property from Plaintiffs, Plaintiffs'

customers, or Plaintiffs' member organizations; (8) misappropriating that which rightfully belongs to Plaintiffs, their customers, or their associated member organizations or in which Plaintiffs', their customers, or their associated member organizations has a proprietary interest; or (9) 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 permanently restrained and enjoined from (1) using and infringing Microsoft's trademarks, including specifically Microsoft's registered trademarks Internet Explorer®, Microsoft®, and Windows®, bearing registration numbers 2872708, 2463526 and 2277112; the trademarks of financial institution members of FS-ISAC and/or other trademarks, trade names, service marks, or Internet Domain addresses or names; (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 Defendants shall forfeit ownership and control of the domains identified in Appendix A to this order to Microsoft.

IT IS FURTHER ORDERED, pursuant to the All Writs Act (28 U.S.C. § 1651), that the domain registries and domain registrars ("Domain Providers") shall transfer ownership of the domains forth in Appendix A to Microsoft. Domain Providers shall implement the provisions of this order in the following fashion:

1. Transfer the domains to the control of Microsoft, such that Microsoft is the registrant with control over hosting and administration of the domains. Domains should be transferred to Microsoft's account at the sponsoring registrar MarkMonitor or such other registrar and account details specified by Microsoft. The domains shall be made active and shall resolve in the manner set forth in this order, or as otherwise be specified by Microsoft, upon its taking control of the domains.

2. The domains shall be assigned the authoritative name servers ns9.microsoftinternetsafety.net and ns10.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name server or taking other reasonable steps to work with Microsoft to ensure that the domains are put within Microsoft's control, and to ensure that Defendants cannot use them to control the botnet.

3. The WHOIS registrant, administrative, billing and technical contact and identifying information should be the following, or other information as may be specified by Microsoft:

Domain Administrator
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
United States
Phone: +1.4258828080
Facsimile: +1.4259367329
domains@microsoft.com

4. The Domain Providers shall prevent transfer or modification of the domains by Defendants and shall prevent transfer or control of the domains to the account of any party other than Microsoft.

5. The Domain Providers shall prevent transfer or modification of the domains by Defendants and shall prevent transfer or control of the domains to the account of any party other than Microsoft.

6. The Domain Providers shall take all steps required to propagate the foregoing changes through the DNS, including domain registrars.

7. Non-U.S. Domain Providers are respectfully requested, but are not ordered, to comply with the foregoing steps, in order to protect the integrity and security of the Internet, to protect end-user victims of the Shylock botnet in all countries, to advance the public interest and to protect Plaintiffs and their customer and members from the Shylock botnet.

8. Third-party The Internet Corporation for Assigned Names and Numbers ("ICANN"), 12025 Waterfront Dr., Suite 300, Los Angeles, California, 90094, is respectfully requested, but is not ordered, to use its best efforts to assist and facilitate the transfer of U.S.-based domains set forth in Appendix A, to Microsoft.

IT IS FURTHER ORDERED that copies of this Order and service of the Complaint may be served by any means authorized by law, including transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their domain registrars and/or hosting companies and as agreed to by Defendants in their domain registration and/or hosting agreements, and/or by publishing notice on a publicly available Internet website.

IT IS SO ORDERED

Entered this ____ day of March, 2015 _____

Liam O'Grady
United States District Judge