CV 15-6565

Katherine L. Maco (4555991)
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, New York, 10019
Telephone: (212) 506-5000

Gabriel Ramsey
(*pro hac vice* application pending)
Jeffrey L. Cox
(*pro hac vice* application pending)
Elena Garcia
(*pro hac vice* application pending)
ORRICK, HERRINGTON & SUTCLIFFE LLP
405 Howard Street
San Francisco, CA 94105-2669
Telephone: (415) 773-5700

Richard Domingues Boscovich
Microsoft Corporation
One Microsoft Way
Redmond, Wa. 98052-6399
Telephone: (425-704-0867)

GLEESON, J.

BLOOM, M.J.

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MICROSOFT CORPORATION, a Washington corporation,

Plaintiff,

v.

JOHN DOES 1-5, CONTROLLING COMPUTER BOTNETS AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS,

Defendants.

Index No.

FILED UNDER SEAL

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

Plaintiff Microsoft Corp. ("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 Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962(c), (d)); and (5) the common law of trespass, unjust enrichment and conversion. 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).

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Microsoft's 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 1-5 ("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 Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962) 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 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 Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962) 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 trademarks "Internet Explorer," "Microsoft," "Windows," "MSN", and "Windows Live" used in connection with its services, software and products.

4. 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 Application for a Temporary Restraining Order, Seizure 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 their claim 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 of Microsoft, without authorization or exceeding authorization, in order to infect those computers and make them part of the computer botnet known as the "Dorkbot" botnet (the "botnet");
b. sending malicious code to configure, deploy and operate a botnet;
c. deploying computers and Internet domains to establish a command and control infrastructure for a botnet;
d. using the command and control servers and Internet domains to actively manage and control a botnet for illegal purposes;
e. corrupting the Microsoft operating system and applications on victims' computers, thereby using them to spy on the victims, spread the Dorkbot infection, propagate additional malicious software, and conduct distributed denial of service attacks on third parties;
f. stealing personal account information and files from computer users; and
g. using stolen information for illegal purposes.

5. 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;

6. 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 Internet domains listed in Appendix A to this Order ("Appendix A") and from the destruction or concealment of other discoverable evidence of Defendants' misconduct available via those domains, including on user computers infected with Dorkbot, 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 botnet command and control software at issue in Microsoft's TRO Application and the harmful, malicious, and trademark infringing software disseminated through the Internet domains listed in Appendix A, thereby permitting them to continue their illegal acts; and

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

7. Microsoft's request for this emergency *ex parte* 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 without prior notice to Defendants, and accordingly, Microsoft is relieved of the duty to provide Defendants with prior notice of Microsoft's motion;

8. 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 New York, 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 Microsoft's customers, to further perpetrate their fraud on Microsoft's customers. There is good cause to believe that Defendants have directed said malicious botnet code and content through certain instrumentalities – specifically the domains and the domain registration facilities of the domain registries identified in Appendix A.

9. 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 botnet code, content, and commands that Defendants use to maintain and operate the botnet to the computers of Microsoft's customers, and to receive the information stolen from those computers.

10. 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.

11. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants must be prohibited from sending malicious botnet code, content and commands from the Internet domains identified in Appendix A to computers of Microsoft's customers.

12. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains identified in Appendix A to host the command and control software and content used to maintain and operate the botnet. There is good cause to believe that to

immediately halt the injury caused by Defendants, each of Defendants' current and prospective domains set forth in Appendix A must be immediately redirected to the Microsoft-secured name-servers named ns085.microsoftinternetsafety.net and ns086.microsoftinternetsafety.net, thus making them inaccessible to Defendants for command and control purposes.

13. There is good cause to believe that to immediately halt the injury, the execution of this Order should be carried out in a coordinated manner by Microsoft and by the domain registries identified in Appendix A on such date and time within ten days of this Order as may be reasonably requested by Microsoft.

14. There is good cause to believe that Defendants will routinely update the Internet domains associated with the Dorkbot botnet, and that Microsoft may identify and update the domains listed in Appendix A as may be reasonably necessary to account for additional Internet domains associated with the Dorkbot botnet just prior to the execution of this Order.

15. 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) by 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 domain registrars and hosting companies and as agreed to by Defendants in their domain registration and/or hosting agreements, (4) publishing notice on a publicly available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

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 Microsoft and the protected computers and operating systems of Microsoft's 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) 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 set forth in Appendix A and through any other component or element of the botnet in any location; (4) stealing information, money, or property from Microsoft or Microsoft's customers; (5) misappropriating that which rightfully belongs to Microsoft, its customers, or in which Microsoft, its customers has a proprietary interest; (6) downloading or offering to download additional malicious software onto the computers of Microsoft's customers; or (6) undertaking any similar activity that inflicts harm on Microsoft, Microsoft'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 "Internet Explorer," "Microsoft," "Windows," "MSN", or "Windows Live" bearing registration numbers 2872708, 2463526, 2277112, 2854091, 3765517 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 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, with respect to any currently registered Internet domains set forth in Appendix A, the domain registries located in the United States shall take the following actions:

A. Maintain unchanged the WHOIS or similar contact and identifying information as of the time of receipt of this Order and maintain the domains with the current registrar;

B. The domains shall remain active and continue to resolve in the manner set forth in this Order;

C. Prevent transfer or modification of the domains by Defendants or third parties at the registrar;

D. The domains shall be redirected to secure servers by changing the authoritative name servers to ns085.microsoftinternetsafety.net and ns086.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 the redirection of the domains and to ensure that Defendants cannot use them to control the botnet.

E. Take all steps required to propagate to the foregoing changes through the Domain Name System ("DNS"), including domain registrars;

F. Preserve all evidence that may be used to identify the Defendants using the domains.

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 domain registrars and registries to execute this order.

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 (1) by 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 domain registrars and/or hosting companies and as agreed to by Defendants in their domain registration and/or 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 December 4, 2015 at _____ 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 $200,000 as cash to be paid into the Court registry.

IT IS FURTHER ORDERED that Microsoft may identify and update the domains in Appendix A to this Order as may be reasonably necessary to account for additional Internet domains associated with the Dorkbot botnet just prior to the execution of this Order.

IT IS FURTHER ORDERED that the Defendants shall file with the Court and serve on Microsoft's counsel any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later than one (1) days prior to the hearing on Microsoft's request for a preliminary injunction.

IT IS SO ORDERED

Entered this ____ day of November, 2015

_____
UNITED STATES DISTRICT JUDGE

APPENDIX A

APPENDIX A

REGISTRY FOR .COM AND .NET DOMAINS

Verisign Naming Services
21345 Ridgetop Circle
4th Floor
Dulles, Virginia 20166
United States

Verisign Global Registry Services
12061 Bluemont Way
Reston Virginia 20190
United States

REGISTRY FOR .INFO DOMAINS

Afilias USA, Inc.
Building 3, Suite 105,
300 Welsh Road, Horsham,
PA 19044
United States

Afilias plc
4th Floor, International House,
3 Harbourmaster Place,
IFSC, Dublin D01 K8F1,
Ireland

CURRENTLY REGISTERED .COM DOMAINS

a350000.com
a36a000.com
a388000.com
a399900.com
a444400.com
aaao2020o.com
alufina.com
b372000.com
b411000.com
b444400.com
baao20221.com
coachloan.com
dacoolair.com
ddoyou4understandme42.com

edoyou5understandme42.com
g4sa.com
girccsas.com
googleure.com
habalot.com
j031333.com
jaao20222.com
jaao20225.com
jo1aa23.com
jo1aa24.com
jo1aa25.com
jo1aa30.com
jo1rv99.com
jo31031.com
jo31032.com
joerv01.com
joerv02.com
joerv06.com
joerv07.com
joerv08.com
k211126.com
k211132.com
k340000.com
laeranat1.com
lartanat1.com
lartanato.com
najwahaifamelema17.com
najwahaifamelema36.com
najwahaifamelema70.com
ratk01.com
retk01.com
rwt234.com
so1aa00.com
sss11c0.com
tassweq.com
tsroxybaa.com
weqband.com
xludakx.com
yamimo.com
yongyuan2.com

CURRENTLY REGISTERED .NET DOMAINS

strongsearch.net
babypin.net
mom002.net
sult4n.net

CURRENTLY REGISTERED .INFO DOMAINS

esta4.info
f0001.info
redflash.info
smellypussy.info
thismynew1.info

DEFENDANTS JOHN DOES 1 – 5 CONTACT INFORMATION

1404418132@qq.com
daliandm@sina.com
esta4.info@protecteddomainservices.com
ewrewr@msn.com
exe445@gmail.com
f0001.info@protecteddomainservices.com
jilaheg@126.com
kdnvkxnxc@sina.com
luanren_8@tom.com
matthew.wen@hotmail.com
mbakerh@yeah.net
qiushangzhi@35.com
ratk01.com@protecteddomainservices.com
trainerlouise@yahoo.com
yuming@yinsibaohu.aliyun.com