

IN CLERK'S OFFICE
U.S. DISTRICT COURT E.D.N.Y.

★ DEC 08 2015 ★

BROOKLYN OFFICE

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

Attorneys for Plaintiff
MICROSOFT CORPORATION

**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. 15-CV-6565 (JG)

ORDER FOR 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, seizure 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 November 23, 2015, the Court granted Microsoft’s Application for an Emergency Temporary Restraining Order, Seizure Order and Order to Show Cause Re Preliminary Injunction (“TRO Application”). Microsoft has executed that order. Microsoft now moves for an Order for Preliminary Injunction seeking to keep in place the relief granted by the November 23rd Order, with respect to the domains attached hereto in Appendix A.¹

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of 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 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),

¹ Pursuant to the Court’s November 23, 2015 Temporary Restraining Order and Order To Show Cause, Microsoft amended Appendix A to the TRO after identifying additional domains functioning as part of the Dorkbot command and control infrastructure. Appendix A to this Proposed Preliminary Injunction Order incorporates those changes.

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. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. There is good cause to believe that the harm to Microsoft of denying the relief requested in their request for a Preliminary Injunction outweighs any harm to any legitimate interests of Defendants and that there is no undue burden to any third party.

13. 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.

PRELIMINARY INJUNCTION

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 (7) 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.

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 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, as this case proceeds.

IT IS FURTHER ORDERED that this Order shall be implemented with the least degree of interference with the normal operation of the domain registries and/or website providers identified in Amended Appendix A.

IT IS SO ORDERED

Entered this 7th day of December, 2015

2:37
P.M.



John Gleeson
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	b372000.com
a36a000.com	b388000.com
a388000.com	b399900.com
a399900.com	b411000.com
a444400.com	b444400.com
aaao2020o.com	baao20221.com
acarakalgroup42.com	baerr02.com
adoyouunderstandme42.com	balkr02.com
aire1bobohayawen42.com	balkr03.com
ajhvdqwladies42.com	bmous2epadsafa42.com
alnisat.com	c35000000.com
alufina.com	c36300000.com
amous1epadsafa42.com	c41100000.com
artiho.com	c44440000.com
b350000.com	coachloan.com
	dacoolair.com

dacoolblr.com
g4sa.com
gircsas.com
googleure.com
habalot.com
hedrmsad.com
j031333.com
j3400000.com
jaao20222.com
jaao20225.com
jaao20226.com
jaao20227.com
jaao29230.com
jaao31231.com
jaao31232.com
jamtes.com
jo1aa23.com
jo1aa24.com
jo1aa25.com
jo1aa27.com
jo1aa30.com
jo1rv99.com
jo31031.com
jo31032.com
joerv01.com
joerv02.com
joerv06.com
joerv07.com
joerv08.com
joyyv02.com
joyyv03.com
k201333.com
k211124.com
k211125.com
k211126.com
k211127.com
k211130.com
k211131.com
k211132.com
k340000.com
laerانات1.com
laerانات2.com
lartانات1.com
lartانات3.com
lartاناتو.com
malaketna.com

najwahai famelema1.com
najwahai famelema100.com
najwahai famelema14.com
najwahai famelema16.com
najwahai famelema17.com
najwahai famelema2.com
najwahai famelema21.com
najwahai famelema28.com
najwahai famelema35.com
najwahai famelema36.com
najwahai famelema37.com
najwahai famelema38.com
najwahai famelema39.com
najwahai famelema40.com
najwahai famelema41.com
najwahai famelema46.com
najwahai famelema47.com
najwahai famelema48.com
najwahai famelema49.com
najwahai famelema5.com
najwahai famelema50.com
najwahai famelema51.com
najwahai famelema52.com
najwahai famelema53.com
najwahai famelema54.com
najwahai famelema55.com
najwahai famelema57.com
najwahai famelema58.com
najwahai famelema59.com
najwahai famelema60.com
najwahai famelema61.com
najwahai famelema7.com
najwahai famelema70.com
najwahai famelema71.com
najwahai famelema72.com
najwahai famelema73.com
najwahai famelema74.com
najwahai famelema75.com
najwahai famelema86.com
najwahai famelema87.com
najwahai famelema88.com
najwahai famelema89.com
najwahai famelema9.com
najwahai famelema91.com
najwahai famelema97.com
najwahai famelema98.com

najwahaifamelema99.com
ratk01.com
retk01.com
rogoeorogico1.com
rooggeyyy1.com
rwt234.com
shaimenal.com
solaa00.com
sss11c0.com
tassweq.com
tsroxybaa.com

weqband.com
xludakx.com
yamimo.com
yongyuan2.com
zabrak0vmin0kov1.com
zabrak0vmin0kov2.com
zabrak0vmin0kov3.com
zabrak0vmin0kov4.com
zabrak0vmin0kov5.com
zabrak0vmin0kov6.com
zabrouskics.com

CURRENTLY REGISTERED .NET DOMAINS

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

CURRENTLY REGISTERED .INFO DOMAINS

esta4.info
f0001.info
ngulesh.info
redflash.info
smelly pussy.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
kdnvkxnc@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