

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division



MICROSOFT CORPORATION, a)
 Washington corporation,)
)
 Plaintiff,)
)
 v.)
)
 JOHN DOES 1-18, CONTROLLING A)
 COMPUTER BOTNET THEREBY)
 INJURING MICROSOFT AND ITS)
 CUSTOMERS)
)
 Defendants.)
)
)
)
)
)

Civil Action No: 1:13cv139 (LMB/TCB)

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)); and (4) the common law of trespass, unjust enrichment and conversion. Microsoft has moved for a preliminary injunction pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C. § 1116(d) (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 Plaintiff's application 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 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) 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), and the Lanham Act (15 U.S.C. §§ 1114, 1125), and that further 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 “Bing,” “Internet Explorer,” “Microsoft,” and “Windows” used in connection with its services, software and products.

4. There is good cause to believe that, unless the 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 and Order to Show Cause Re Preliminary Injunction (“Preliminary Injunction 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 code to Microsoft’s and its customers’ protected computers and Windows operating systems, without authorization and exceeding authorization, in order to infect those computers and make them part of the botnet;
- b. sending malicious code to configure, deploy and operate a botnet;
- c. taking control of internet search engine results, including results provided by Microsoft’s Bing search engine, and redirecting clicks on those results to locations different from those intended by Microsoft and its customers, without their authorization or consent;

- d. taking control of Microsoft's Internet Explorer browser and generating clicks through that browser without the authorization or consent of Microsoft or its customers;
- e. creating unauthorized versions and instances of Microsoft's Internet Explorer browser, thereby creating unauthorized copies of Microsoft's Internet Explorer trademark and falsely indicating that such versions and instances of Internet Explorer are associated with or approved by Microsoft, the purpose of which is to deceive customers;
- f. creating unauthorized versions and instances of Microsoft's Bing Search engine web page and functionality, thereby creating unauthorized copies of Microsoft's Bing trademark and falsely indicating that such versions and instances of the Bing search engine are associated with or approved by Microsoft, the purpose of which is to deceive customers;
- g. creating and redirecting Microsoft's customers to websites containing unauthorized copies of Microsoft's trademarks, without the authorization or consent of Microsoft or its customers, and falsely indicating that such websites are associated with or approved by Microsoft, the purpose of which is to deceive customers;
- h. collecting personal information without authorization and content, including personal search engine queries and terms; and
- i. delivering malicious code.

5. There is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft, its 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 Protocol (IP) addresses listed in Appendix B and the Internet domains and subdomains listed in Appendices A, B and C, and from the destruction or concealment of other discoverable evidence of Defendants' misconduct available at those locations if Defendants receive advance notice of this action. Based on the evidence cited in Microsoft's Preliminary Injunction 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 harms Microsoft, its customers and the public;
- b. Defendants have continued their unlawful conduct despite the clear injury to Microsoft, its customers, and the public;
- c. Defendants are likely to delete or relocate the harmful, malicious and trademark infringing botnet command and control software at issue in Microsoft's Preliminary Injunction Application, which is operating at and disseminated through the IP addresses and domains and subdomains at issue, and to destroy information and evidence of their misconduct stored at the IP addresses, domains and subdomains; 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 relief is not the result of any lack of diligence on Microsoft's part, but instead is based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), 15 U.S.C. § 1116(d) and 28 U.S.C. § 1651(a), good cause and the interest of justice require that this Order be Granted;

8. There is good cause to believe that Defendants have specifically directed their activities to the computers of Microsoft's customers located in the Eastern District of Virginia, and have engaged in illegal activity using IP addresses at Leaseweb, with a presence in the Eastern District of Virginia, and various ".com," ".org" and ".cc" domains (among others) that

are maintained by the top level domain registries Verisign and Public Interest Registry, located in the United States and the Eastern District of Virginia.

9. There is good cause to believe that Defendants have engaged in illegal activity using the data centers and/or Internet hosting providers identified in Appendix B to host the command and control software and the malicious botnet code and content used to maintain and operate the botnet at computers, servers, electronic data storage devices or media at the IP addresses identified in Appendix B.

10. There is good cause to believe that to immediately halt the injury caused by Defendants, data and evidence at the IP addresses identified in Appendix B must be preserved and held in escrow pending further order of the court, Defendants' computing resources related to such IP addresses must then be disconnected from the Internet, Defendants must be prohibited from accessing Defendants' computer resources related to such IP addresses and the data and evidence located on those computer resources must be secured and preserved.

11. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains and subdomains identified in Appendices A, B and C 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 immediately halt the injury caused by Defendants, each of Defendants' current and prospective domains and subdomains set forth in Appendices A, B and C must be immediately redirected to secure servers by changing the authoritative name servers to ns3.microsoftinternetsafety.net and ns4.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name server ns3.microsoftinternetsafety.net to 157.56.78.93 and the IP address associated with name server ns4.microsoftinternetsafety.net to 157.56.78.73 or taking other reasonable steps to work with Microsoft to ensure the redirection of the domains and subdomains and to ensure that Defendants cannot use them to control the botnet.

12. There is good cause to believe that to immediately halt the injury caused by Defendants, an HTML webpage should be presented at the redirected domains and subdomains,

informing victims that their computers are infected with the malicious botnet software and providing instructions allowing them to remove the malicious software if they elect to do so.

13. There is good cause to permit notice of the instant Order 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, satisfy Fed. R. Civ. Pro. 4(f)(3), and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided contact information in foreign countries that are signatory to such treaties; (2) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their domain name registrars and to subdomain services and as agreed to by Defendants in their domain name or subdomain registration agreements; and (3) publishing notice on a publically available Internet website.

PRELIMINARY INJUNCTION

IT IS THEREFORE ORDERED that, Defendants, their representatives and persons who are in active concert or participation with them are restrained and enjoined from (1) intentionally accessing and sending malicious software or code to Microsoft's and its customers protected computers and Windows operating systems, 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) taking control of internet search engine results or browsers, including Microsoft's Bing search engine and Internet Explorer browser; (4) redirecting search engine results or browser activities or generating unauthorized "clicks;" (5) collecting personal information including search terms and keywords; (6) configuring, deploying, operating or otherwise participating in or facilitating the botnet described in the Preliminary Injunction Application, including but not limited to the command and control software hosted at and operating through the IP addresses, domains and subdomains set forth herein and through any other component or element of the botnet in any location; (7) misappropriating that which

rightfully belongs to Microsoft or its customers or in which Microsoft has a proprietary interest; or (8) undertaking similar activity that inflicts harm on Microsoft, its 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 "Bing," "Internet Explorer," "Microsoft" or "Windows," bearing registration numbers 2872708, 2463526, 2277112 and 3883548; (2) creating unauthorized copies, versions and instances of Microsoft's Internet Explorer browser, Bing search engine, and trademarks or falsely indicating that Microsoft is associated with or approves the foregoing; (3) 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 (4) 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 domains and subdomains set forth in Appendices A, B and C, the domain registries, subdomain services and registrants, 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 and subdomains with the current registrar or subdomain service;

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

C. Prevent transfer or modification of the domains and subdomains by Defendants or third parties at the registrar and/or subdomain services;

D. The domains and subdomains shall be redirected to secure servers by changing the authoritative name servers to ns3.microsoftinternetsafety.net and ns4.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name server ns3.microsoftinternetsafety.net to 157.56.78.93 and the IP address associated with name server ns4.microsoftinternetsafety.net to 157.56.78.73 or taking other reasonable steps to work with Microsoft to ensure the redirection of the domains and subdomains 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 DNS, including domain registrars and/or subdomain services;

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

IT IS FURTHER ORDERED that, with respect to any domains and subdomains set forth in Appendices A, B and C that are currently unregistered, the domain registries, subdomain services and registrants shall take the following actions:

A. Transfer the domains and subdomains to the control of Microsoft, such that Microsoft is the registrant with control over hosting and administration of the domains and subdomains. Domains should be transferred to Microsoft's account at the sponsoring registrar MarkMonitor.

B. The WHOIS registrant, administrative, billing and technical contact and identifying information should be the following;

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

C. The domains and subdomains shall be made active and shall resolve in the manner set forth in this order or as otherwise specified by Microsoft.

D. The domains and subdomains shall be assigned the authoritative name servers ns3.microsoftinternetsafety.net and ns4.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name server ns3.microsoftinternetsafety.net to 157.56.78.93 and the IP address associated with name server ns4.microsoftinternetsafety.net to 157.56.78.73 or taking other reasonable steps to work with Microsoft to ensure that the domains and subdomains are put within Microsoft's control, and to ensure that Defendants cannot use them to control the botnet.

IT IS FURTHER ORDERED that Defendants' materials bearing the infringing marks, the means of making the counterfeit marks, materials involved in making and using the counterfeit marks, and associated records, including all computers, servers, electronic data storage devices or media associated with Defendants' IP addresses at the hosting companies set forth in Appendix B, shall be disconnected from the Internet, preserved and held by substitute custodian Nardello & Co. LLC, 1111 Brickell Avenue, 11th Fl., Miami, FL 33131.

IT IS FURTHER ORDERED that, with respect to the IP addresses in Appendix B, the Internet hosting providers shall:

A. Take all reasonable steps necessary to completely block all access to the IP addresses set forth in Appendix B by Defendants, Defendants' representatives, resellers, and any other person or computer, except as explicitly provided for in this Order;

B. Completely disable the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with the IP addresses set forth in Appendix B and make them inaccessible from any other computer on the Internet, any internal network, or in any other manner, to Defendants, Defendants' representatives and all other persons, except as otherwise ordered herein;

C. Completely, and until further order of this Court, suspend all services associated with the IP addresses set forth in Appendix B;

D. Not enable, and shall take all reasonable steps to prevent, any circumvention of this order by Defendants or Defendants' representatives associated with the IP addresses or any other person;

E. Disable and deny to Defendants and Defendants' representatives, access to any and all "backup" systems, arrangements or services that might otherwise be used to support the IP addresses set forth in Appendix B or that might otherwise be used to circumvent this Order;

F. Log all attempts to connect to or communicate with the IP addresses set forth in Appendix B;


G. Preserve, retain and produce to Microsoft all documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling the IP addresses set forth in Appendix B, including any and all individual or entity names, mailing addresses, e-mail addresses, facsimile numbers and telephone numbers or similar contact information, including but not limited to such contact information reflected in billing, usage, access and contact records and all records, documents and logs associated with Defendants' or Defendants' Representatives' use of or access to the IP addresses.

IT IS FURTHER ORDERED that copies of this Order, notice of this Order and service of the Complaint may be served by any means authorized by law, including (1) by personal delivery upon Defendants who provided contact information in the U.S.; (2) personal delivery through the Hague Convention on Service Abroad upon Defendants who provided contact information outside the U.S.; (3) by transmission by e-mail, facsimile and mail to the contact information provided by Defendants to the data centers, Internet hosting providers, domain registrars and subdomain service providers who hosted the software code associated with the domains and IP addresses set forth at Appendices A, B and C; and (4) by publishing notice to Defendants on a publicly available Internet website.

IT IS FURTHER ORDERED, that the relief set forth herein shall remain in effect during the pendency of the above-captioned action.

IT IS SO ORDERED

Entered this 13th day of February, 2013.

lsl 

Leonie M. Brinkema
United States District Judge