IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

MICROSOFT CORPORATION, a Washington Corporation, Plaintiff v. JOHN DOES 1-8 CONTROLLING A COMPUTER BOTNET THEREBY INJURING MICROSOFT AND ITS CUSTOMERS, Defendants.	§	CASE NO: **FILED UNDER SEAL** A13CV1014 SS

[~~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)); and (4) 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 - 8 ("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), the Lanham Act (15 U.S.C. §§ 1114, 1125) 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 "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 ("TRO 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 computer botnet known as the "ZeroAccess" botnet (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 malicious software or 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 and Internet domains listed in Appendix A to this Order 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 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 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 TRO Application, which is operating at and disseminated through the IP addresses and domains at issue, and to destroy information and evidence of their misconduct stored at the IP addresses and domains; 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 Western District of Texas, have engaged in illegal activity using IP addresses identified in Appendix A to this Order that are

registered to command and control servers located at hosting companies in Germany, Latvia, the Netherlands, Switzerland and Luxembourg (set forth in Appendix A), and have engaged in illegal activity by using the domains identified in Appendix A, by directing malicious botnet code and content to said computers of Microsoft's customers. There is good cause to believe that Defendants have directed said malicious botnet code and content through certain instrumentalities – specifically the computer networks of the Internet Service Providers (ISPs) identified in Appendix B to this Order that Microsoft's customers use to access the Internet, and the hosting companies and domain registries identified in Appendix A to this Order.

9. There is good cause to believe that Defendants have engaged in illegal activity by using the networks of the ISPs identified in Appendix B and the hosting facilities and domain registration facilities of the companies in Appendix A, to deliver from the IP Addresses and domains identified in Appendix A, the malicious botnet code and content that Defendants use to maintain and operate the botnets to the computers of Microsoft's' customers.

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 and content from the IP Addresses identified in Appendix A to computers of Microsoft's customers. There is good cause to believe that to immediately halt the injury caused by Defendants, the ISPs identified in Appendix B and the hosting companies identified in Appendix A should take steps to block incoming and/or outgoing traffic on their respective networks that originates or has been sent from and/or to the IP Addresses identified in Appendix A such that said traffic will not reach victim end-user computers on the ISPs' respective networks and/or the computers at the IP Addresses in Appendix A.

11. There is good cause to believe that Defendants have engaged in illegal activity using the IP Addresses 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 in order to immediately halt the injury caused by Defendants and to ensure the future prosecution of this case it not rendered fruitless by attempts to delete, hide, conceal, or otherwise render

inaccessible the software components that create, distribute, and are involved in the creation, perpetuation, and maintenance of the botnet and prevent the creation and distribution of unauthorized copies of Microsoft's registered trademarks and carry out other harmful conduct, with respect to the Defendants' most current, active command and control servers hosted at the IP Addresses, the following actions should be taken. The ISPs identified in Appendix B and the hosting companies identified in Appendix A should block incoming and/or outgoing traffic on their respective networks that originates or has been sent from and/or to the IP Addresses identified in Appendix A, such that said traffic will not reach victim end-user computers on the ISPs' respective networks and/or the computers at the IP Addresses in Appendix A, and should take other reasonable steps to block such traffic to and/or from any other IP addresses to which Defendants may move the botnet infrastructure, identified by Microsoft and which the Court may order to be subject to this Order, to ensure that Defendants cannot use such infrastructure to control the botnet.

12. 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 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 NS1.microsoftinternetsafety.net and NS2.microsoftinternetsafety.net and thus made inaccessible to Defendants.

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 ISPs identified in Appendix B to this Order and the domain registries and hosting companies identified in Appendix A to this Order on or about 10:00 a.m. Central Standard Time on December 5, 2013, or such other date and time within eight days of this order as may be reasonably requested by Microsoft.

14. 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, 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 hosting companies and as agreed to by Defendants in their 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'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 TRO Application, including but not limited to the command and control software hosted at and operating through the IP addresses 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 the IP Addresses set forth in Appendix A to this Order, the ISPs identified in Appendix B to this Order shall take reasonable best efforts to implement the following actions:

A. Without the need to create logs or other documentation, identify incoming and/or outgoing Internet traffic on their respective networks that originates and/or is being sent from and/or to the IP Addresses identified in Appendix A that is directed to and/or from computers that connect to the Internet through the ISPs' respective networks;

B. Block incoming and/or outgoing Internet traffic on their respective networks that originate and/or are being sent from and/or to the IP Addresses identified in Appendix A that is directed to and/or from computers that connect to the Internet through the ISPs' respective networks;

C. Take other reasonable steps to block such traffic to and/or from any other IP addresses to which Defendants may move the botnet infrastructure, identified by Microsoft and which the Court may order to be subject to this Order, to ensure that Defendants cannot use such infrastructure to control the botnet.

D. 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 hosting companies or other ISPs to execute this order;

E. Take all reasonable steps necessary to block the IP Addresses in Appendix A, as set forth above, so to prevent Defendants or Defendants' representatives or any other person, from accessing the IP Addresses, except as explicitly provided for in this Order;

F. Not enable, and shall take all reasonable steps to prevent, any circumvention of this order by Defendants, Defendants' representatives or any other person;

G. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order;

IT IS FURTHER ORDERED that, with respect to the IP Addresses in Appendix A, the non-U.S. hosting companies set forth at Appendix A are respectfully requested, but not ordered, to comply with the following steps, in order to protect the integrity and security of the Internet, to protect the hosting companies' own systems, to protect end-user victims of the botnet in all countries, to advance the public interest and to protect Microsoft and its customers from the botnet:

A. Take all reasonable steps necessary to completely block all access to and all traffic to and from the IP Addresses set forth in Appendix A 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 A 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 A;

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. Log all attempts to connect to or communicate with the IP Addresses set forth in Appendix A;

F. 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 A, 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.

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 explicitly provided for in this Order;

H. Transfer any content and software hosted at the IP Addresses listed in Appendix A that are not associated with Defendants, if any, to new IP Addresses not listed in Appendix A; notify any non-party owners of such action and the new IP addresses, and direct them to contact Microsoft's counsel, Gabriel M. Ramsey, Orrick Herrington & Sutcliffe, 1000 Marsh Road, Menlo Park, CA 90425-1015, gramsey@orrick.com, (Tel: 650-614-7400), to facilitate any follow-on action;

I. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order.

IT IS FURTHER ORDERED that, with respect to any *currently registered* 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 NS1.microsoftinternetsafety.net and NS2.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 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, with respect to any domains set forth in Appendix A that are *currently unregistered*, the domain registries and registrars located in the United States shall take the following actions:

A. 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.

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

D. The domains shall be assigned the authoritative name servers NS1.microsoftinternetsafety.net and NS2.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name servers or taking such 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.

E. 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 or 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 hosting companies and as agreed to by Defendants in their 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 12th, 2013 at 9:30 AM 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 $250,000 as cash to be paid into the Court registry.

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 two (2) days prior to the hearing on Microsoft's request for a preliminary injunction. Microsoft may file responsive or supplemental pleadings, materials, affidavits, or memoranda with the Court and serve the same on counsel for the Defendants no later than one (1) day prior to the preliminary injunction hearing in this matter. Provided that service shall be performed by personal or overnight delivery, facsimile or electronic mail, and documents shall be delivered so that they shall be received by the other parties no later than 4:00 p.m. (Central Standard Time) on the appropriate dates listed in this paragraph.

IT IS SO ORDERED

Entered this 25th day of November, 2013.

Barbara Parks
United States District Judge