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

MICROSOFT CORPORATION, a Washington corporation,

Plaintiff,

v.

DOMINIQUE ALEXANDER PATTI, an individual; DOTFREE GROUP S.R.O., a Czech limited liability company, JOHN DOES 1-22, CONTROLLING A COMPUTER BOTNET THEREBY INJURING MICROSOFT AND ITS CUSTOMERS

Defendants.

Civil Action No: 1:11cv1017

FILED UNDER SEAL

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

Plaintiff Microsoft Corp. ("Microsoft") has file a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) the CAN-SPAM Act (15 U.S.C. § 7704); (3) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); and (4) the common law of trespass, unjust enrichment, conversion, and negligence. 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 and the All-Writs Act, 28 U.S.C. § 1651.

FINDINGS

The Court has considered the pleadings, declarations, exhibits, and memorandum filed in support of Microsoft's motion and finds that:

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 thereto; the Complaint states a

claim upon relief may be granted against Defendants under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125), common law trespass to chattels, unjust enrichment, conversion, and negligence.

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), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125), common law trespass to chattels, unjust enrichment, conversion, and negligence, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. 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 of the Computer Fraud and Abuse Act (18 U.S.C. § 1030), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125), common law trespass to chattels, unjust enrichment, conversion, and negligence. 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 Motion"), 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 operating systems, without 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. sending unsolicited spam email to Microsoft's Hotmail accounts;

d. collecting personal information, including personal email addresses; and

e. delivering malicious code.

4. 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;

5. 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 the IP addresses and Internet domains at issue in Microsoft's TRO Motion and other discoverable evidence of Defendants' misconduct available through such IP addresses and Internet domains if the Defendants receive advance notice of this action. Based on the evidence cited in Microsoft's TRO Motion 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 relocate the information and evidence of their misconduct stored at the IP addresses and Internet domains at issue in Microsoft's TRO Motion and the harmful and malicious code disseminated through these IP addresses and Internet domains; and

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

6. 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), Civil L.R. 65-1 and the All-Writs Act, 28 U.S.C. § 1651, 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;

7. There is good cause to believe that Defendants have engaged in illegal activity using the IP addresses and the .com and .cc domains that are maintained by the top level domain registry Verisign, located in the United States and the Eastern District of Virginia.

8. There is good cause to believe that to immediately halt the injury caused by Defendants, the hosting companies, IP registries, domain registries and domain registrars set forth in Appendices A and B, must be ordered, at 3:00 a.m. Eastern Daylight Time on September 26, 2011 or such other date and time as requested by Microsoft within seven days of this Order:

a. to immediately take all steps necessary to lock at the registry level the domains at issue in the TRO Motion, and which are set forth at Appendix A hereto, to ensure that changes to the domain names cannot be made absent a court order;

b. to immediately take all steps required to propagate the foregoing domain registry changes to domain name registrars; and

c. to hold the domains in escrow and take all steps necessary to ensure that the evidence of misconduct available through the domains be preserved.

d. to immediately take all steps necessary to disable access to the IP addresses at issue in the TRO Motion, and which are set forth at Appendix B hereto, to ensure that access to the IP addresses cannot be made absent a court order;

9. 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. 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, (3) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their domain name registrars and as agreed to

by Defendants in their domain name registration agreements, (4) publishing notice on a publically 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 and their representatives are temporarily restrained and enjoined from intentionally accessing and sending malicious software or code to Microsoft's and its customers protected computers and operating systems, without authorization, in order to infect those computers and make them part of the Kelihos botnet, sending malicious code to configure, deploy and operate a botnet, sending unsolicited spam email to Microsoft's email and messaging accounts and services, sending unsolicited spam email that falsely indicates that they originated from Microsoft or are approved by Microsoft or are from its email and messaging accounts or services, collecting personal information including personal email addresses, delivering malicious code including fake antivirus software, or undertaking similar activity that inflicts harm on Microsoft, its customers, or the public.

IT IS FURTHER ORDERED that, Defendants and their representatives are temporarily restrained and enjoined from configuring, deploying, operating or otherwise participating in or facilitating the botnet described in the TRO Motion, including but not limited to the command and control software hosted at and operating through the IP addresses and domains set forth herein and through any other component or element of the botnet in any location.

IT IS FURTHER ORDERED that Defendants and their representatives are temporarily restrained and enjoined from using the "Microsoft," "Windows," "Hotmail," "Windows Live" and "MSN" trade names, trademarks or service marks, in Internet Domain addresses or names, in content or in any other infringing manner or context, or acting in any other manner which suggests in any way that Defendants' products or services come from or are somehow sponsored or affiliated with Microsoft, and from otherwise unfairly competing with Microsoft, misappropriating that which rightfully belongs to Microsoft, or passing off their goods as Microsoft's.

IT IS FURTHER ORDERED that the domain registries and registrars set forth in Appendix A must:

a. immediately take all steps necessary to lock at the registry level the domains at issue in the TRO Motion, an which are set forth at Appendix A hereto, to ensure that changes to the domain names cannot be made absent a court order;

b. immediately take all steps required to propagate to the foregoing domain registry changes to domain name registrars; and

c. hold the domains in escrow and take all steps necessary to ensure that the evidence of misconduct available through the domains be preserved.

d. Shall completely refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and shall refrain from publicizing this Order until this Order is executed in full, except as explicitly provided for in this Order;

a. Shall save all communications to or from Defendants or Defendants' Representatives and/or related to the domains set forth in Appendix A;

e. Shall preserve and retain all records and documents associated with Defendants' or Defendants' Representatives' use of or access to the domains set forth in Appendix A, including billing and contact information relating to the Defendants or Defendants' representatives using these servers and all logs associated with these servers.

IT IS FURTHER ORDERED that the Internet hosting and service providers identified in Appendix B to this order:

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

c. Shall immediately and 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;

d. Shall immediately, completely, and until further order of this Court, suspend all services associated with the IP addresses set forth in Appendix B;

e. Shall 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;

f. Shall disable, and shall 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;

g. Shall log all attempts to connect to or communicate with the IP addresses set forth in Appendix B;

h. Shall save all communications to or from Defendants or Defendants' Representatives and/or related to the IP addresses set forth in Appendix B;

i. Shall preserve and retain all records and documents associated with Defendants' or Defendants' Representatives' use of or access to the IP addresses set forth in Appendix B, including billing and contact information relating to the Defendants or Defendants' representatives using these servers and all logs associated with these servers;

j. Shall completely refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and

shall refrain from publicizing this Order until this Order is executed in full, except as explicitly provided for in this Order;

IT IS FURTHER ORDERED that Internet hosting and service providers identified in Appendix B to this Order:

a. Shall immediately identify and create a written list of domains, if any, hosted at the IP addresses set forth in Appendix B; shall transfer any content and software associated with such domains to IP addresses not listed in Appendix B; and shall notify the domain owners of the new IP addresses, and direct the domain owners to contact Microsoft's Counsel, Gabriel M. Ramsey, Orrick Herrington & Sutcliffe, 1000 Marsh Road, Menlo Park, CA 90425-1015, (Tel: 650-614-7400), to facilitate any follow-on action.

b. Shall produce to Microsoft 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 and contact records.

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 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 and domain registrars who hosted the software code associated with the domains and IP addresses set forth at Appendices A and B; and (4) by

publishing notice to Defendants on a publicly available Internet website and/or in newspapers in the communities in which 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 ~~within 14 days from the date of this order~~ on October 5th 2011 at 10:30 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 $10,000 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 four (4) 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. (Eastern Standard Time) on the appropriate dates listed in this paragraph.

IT IS SO ORDERED

Entered this 22nd day of September, 2011.

10:14 A.M. E.D.T.

/s/
James C. Cacheris
United States District Judge

United States District Judge