EXHIBIT 32

IN THE UNITED STATES DISTRICT COURT

FOR THE WESTERN DISTRICT OF NORTH CAROLINA

CHARLOTTE DIVISION

MICROSOFT CORPORATION,
Plaintiff,
v.
JOHN DOES 1-82, CONTROLLING A COMPUTER BOTNET THEREBY INJURING MICROSOFT AND ITS CUSTOMERS,
Defendants.

FILED UNDER SEAL

Civil Action No. 3:13cv319

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

Plaintiff Microsoft Corp. ("Microsoft" or "Plaintiff") has filed a Complaint for injunctive and other relief pursuant to, the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the CAN-SPAM Act (15 U.S.C. § 7704); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); North Carolina General Statute § 14-458 (Computer Trespass); and the common law of conversion, unjust enrichment and nuisance. Plaintiff has also moved *ex parte* for an emergency temporary restraining order and seizure order 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"), and an order to show cause why a preliminary injunction should not be granted.

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Plaintiff's Application for an Emergency Temporary Restraining Order, Seizure Order,

and Order to Show Cause for Preliminary Injunction ("TRO Application"), 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); the CAN-SPAM Act (15 U.S.C. § 7704); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); North Carolina General Statute § 14-458 (Computer Trespass); and the common law of conversion, unjust enrichment and nuisance.

2. Microsoft owns the registered trademarks "Microsoft," "Windows," and "Internet Explorer," used in connection with its services, software, and products. Trademarks of third parties and other members of the public are also impacted by Defendants' activities.

3. 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); the CAN-SPAM Act (15 U.S.C. § 7704); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); North Carolina General Statute § 14-458 (Computer Trespass); and the common law of conversion, unjust enrichment and nuisance.

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 Defendants' ongoing violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the CAN-SPAM Act (15 U.S.C. § 7704); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); North Carolina General Statutes § 14-458 (Computer Trespass); and the common law of conversion, unjust enrichment and nuisance. The evidence set forth in Plaintiff's TRO Application and the accompanying declarations and exhibits, demonstrates that Plaintiff is likely to prevail on its claim that Defendants have engaged in violations of the foregoing laws by:

a. Developing, commercializing, and supporting a Citadel botnet development kit, with the purpose and effect of enabling other Defendants to create, deploy, and operate, Citadel botnets with the purpose of stealing identification and personal security information and money, intruding upon Microsoft's software and its customers' computers, and intruding upon the protected computers of third parties, including banks and other members of the public;

b. Providing a stolen version of Windows XP and a stolen Windows XP product key with the sole purpose and effect of enabling other Defendants to create, deploy, and operate, criminal botnets with the purpose of stealing identification and personal security information and money, and intruding upon Microsoft's software and its

customers' computers;

c. Creating, deploying, and operating criminal botnets with the purpose and effect of stealing identification and personal security information and money through the misuse of Plaintiff's Windows operating system and Internet Explorer software;

d. Intentionally accessing and sending malicious software to Microsoft's licensed Windows operating system and Internet Explorer software, the protected computers of Microsoft's customers and also the protected computers of third parties, including banks and other members of the public, without authorization, in order to infect those computers and make them part of the Citadel botnet;

e. Sending malicious software to configure, deploy and operate a botnet;

f. Sending unsolicited spam e-mail to Microsoft's Hotmail accounts;

g. Sending unsolicited spam e-mails that falsely indicate that they are from or approved by Plaintiff or third-parties, including banks, NACHA or other companies or institutions, the purpose of which is to deceive computer users into taking steps that will result in the infection of their computers with botnet code and/or the disclosure of personal and financial account information;

h. Stealing personal and financial account information from users of Microsoft's Windows operating system and Internet Explorer software;

i. Using stolen information to steal money from the financial accounts of

those users using Microsoft's Windows operating system and Internet Explorer software; and

j. Associating with one another in a common criminal enterprise engaged in these illegal acts.

5. There is good cause to believe that if such conduct continues, irreparable harm will occur to Plaintiff and the public, including Plaintiff's customers, financial institutions, NACHA and other members of the public.

6. There is good cause to believe that the Defendants are engaging, and will continue to engage, in such unlawful actions if not immediately restrained from doing so by Order of this Court. 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 botnet command and control software that is hosted at and otherwise operates through the Internet domains listed in Appendix A and the Internet Protocol (IP) addresses listed in Appendix B, 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.

7. There is good cause to believe that, based on the evidence cited in Plaintiff's TRO Application and accompanying declarations and exhibits, Plaintiff is likely to be able to prove that: (1) Defendants are engaged in activities that directly violate U.S. law and harm Plaintiff and the public, including Plaintiff's customers and third party financial institutions, NACHA and other members of the public; (2) Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests; (3) Defendants are likely to delete or relocate the botnet command and control software at issue in Plaintiff's TRO Application

and the harmful, malicious, and trademark infringing software disseminated through these IP addresses and domains and to warn their associates engaged in such activities if informed of Plaintiff's action.

8. There is good cause to believe that Plaintiff's request for this emergency *ex parte* relief is not the result of any lack of diligence on Plaintiff's part, but instead is based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b) and 15 U.S.C. § 1116(d), good cause and the interests of justice require that this Order be granted without prior notice to Defendants, and accordingly Plaintiff is relieved of the duty to provide Defendants with prior notice of Plaintiff's motion.

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, Defendants' data and evidence at Defendants' IP addresses at the data centers and/or Internet hosting providers identified in Appendix B must be preserved and held in escrow pending further order of the court, Defendants' computing resources related to malicious domains hosted at 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. There is good cause to believe that Defendants must be ordered not to use all IP addresses known to have been associated with the botnets at issue in this case,

listed at Appendix B.

11. There is good cause to believe that to immediately halt the injury caused by Defendants, and to ensure that future prosecution of this case is not rendered fruitless by attempts to delete, hide, conceal, or otherwise render inaccessible the software components that distribute unlicensed copies of Plaintiff's registered trademarks and carry out other harmful conduct, with respect to Defendants' most current, active command and control IP addresses hosted at data centers operated by Linode LLC/Linode VPS Hosting and Network Operations Center, Inc./BurstNET Technologies, Inc., the Federal Bureau of Investigation and the United States Marshals Service in the judicial districts where the data centers are located should be directed to seize, impound and deliver into the custody of third-party escrow service Stroz Friedberg, 1925 Century Park East, Suite 1350, Los Angeles, CA 90067, all of Defendants' computers, servers, electronic data storage devices, software, data or media, or copies thereof, associated with the IP addresses at those facilities listed in Appendix B.

12. There is good cause to believe that the Citadel malicious software code infecting end-user computers poses a significant and present threat to those end-users as well as to third party financial institutions with which those end-users maintain their financial accounts, and that therefore, both the end-users and the financial institutions victimized by the Citadel malicious software would stand to benefit through the neutralization and removal of the Citadel malicious software from the end-users' computers.

13. There is good cause to believe that Citadel malicious software code infecting end-user computers keeps those computers from connecting to the websites of providers of anti-virus software and updating the anti-virus software on their computer, thereby

subjecting the computers to the threat of repeated malware infections, unless steps are taken to alter the behavior of the Citadel malicious software or remove it entirely.

14. There is good cause to believe that the Citadel malicious code infecting end-user computers will continue to monitor the Internet browsing activities of those computers unless steps are taken to alter its behavior or remove it entirely.

15. 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 NS5.microsoftinternetsafety.net and NS6.microsoftinternetsafety.net and thus made inaccessible to Defendants.

16. There is good cause to direct that third party Internet registries, data centers, and hosting providers with a presence in the United States to reasonably assist in the implementation of this Order and refrain from frustrating the implementation and purposes of this Order, pursuant to 28 U.S.C. § 1651(a) (the All Writs Act).

17. There is good cause to believe that if Defendants are provided advance notice of Plaintiffs' TRO Application or this Order, they would move the botnet infrastructure, allowing them to continue their misconduct and that they would destroy, move, hide, conceal, or otherwise make inaccessible to the Court evidence of their misconduct, the botnet's activity, the infringing materials, the instrumentalities used to make the infringing materials, and the records evidencing the manufacture and distributing of the infringing materials.

18. 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) transmission by e-mail, electronic messaging addresses, facsimile, and mail to the known email and messaging addresses of Defendants and to their contact information provided by Defendants to the domain registrars, registries, data centers and Internet hosting providers, who host the software code associated with the IP addresses in Appendix B, or through which domains in Appendix A are registered; (2) personal delivery upon Defendants who provided to the data centers and Internet hosting providers contact information in the U.S.; (3) personal delivery through the Hague Convention on Service Abroad or other treaties upon Defendants who provided contact information outside the United States; and (3) publishing notice to the Defendants on a publicly available Internet website. Further, given the high degree of harm to the public caused by Defendants' actions, there is good cause to permit Plaintiff to otherwise publicize its actions to neutralize the Citadel botnet by appropriate means following the unsealing of this Matter.

19. There is good cause to believe that the harm to Plaintiff of denying the relief requested in its TRO Application outweighs any harm to any legitimate interests of Defendants and that there is no undue burden to any third party.

TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

IT IS THEREFORE ORDERED as follows:

A. 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 to Plaintiff, its protected Windows operating system and Internet Explorer software, the protected computers of Plaintiff's customers and to the computers of third-party financial institutions and other members of the public, without authorization, in order to infect those computers and make them part of the botnet; (2) sending malicious software to configure, deploy and operate a botnet; (3) sending unsolicited spam e-mail to Microsoft's Hotmail accounts; (4) sending unsolicited spam e-mail that falsely indicate that they are from or approved by Plaintiff or third-parties, including financial institutions, NACHA and other companies and institutions; (5) creating false websites that falsely indicate that they are associated with or approved by Plaintiff or third-party financial institutions; or (6) stealing information, money or property from Plaintiff, Plaintiff's customers or third-party financial institutions and other members of the public, or undertaking any similar activity that inflicts harm on Plaintiff, or the public, including Plaintiff's customers, financial institutions and NACHA.

B. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from configuring, deploying, operating or otherwise participating in or facilitating the botnets described in the TRO Application, including but not limited to the command and control software hosted at and operating through the domains and IP addresses set forth herein and through any other component or element of the botnets in any location.

C. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from using Plaintiff's

trademarks "Microsoft," "Windows," "Internet Explorer," and the trademarks of third parties including "NACHA," the NACHA logo, trademarks of financial institutions and/or other trademarks; trade names; service marks; or Internet Domain addresses or names; 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 Plaintiff or other companies or institutions, and from otherwise unfairly competing with Plaintiff, misappropriating that which rightfully belongs to Plaintiff or Plaintiff's customers or third-parties, including financial institutions, NACHA or other members of the public, or passing off their goods or services as Plaintiff's or as those of third-parties, including financial institutions, NACHA or other members of the public.

D. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from infringing Plaintiffs' registered trademarks, Registration Nos. 2872708 ("Microsoft"), 2463510 ("Windows") 2277112 ("Internet Explorer") and others.

E. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from using in connection with Defendants' activities any false or deceptive designation, representation or description of Defendants' or of their representatives' activities, whether by symbols, words, designs or statements, which would damage or injure Plaintiff or give Defendants an unfair competitive advantage or result in deception of consumers.

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 NS5.microsoftinternetsafety.net and NS6.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.

H. With regard to the domain registries and registrars located outside of the United States, the Court respectfully requests, but does not order, that they take the same or substantially similar actions so as to neutralize the threat posed by the Citadel botnet to the citizens and financial institutions of all countries, including their own. Defendants, their representatives and

persons who are in active concert or participation with them are ordered to consent to whatever actions are necessary for non-United States registries, registrars and registrants or hosts to effectuate this request.

IT IS FURTHER ORDERED that, with respect to any domains set forth in Appendix A that are *currently unregistered*, the domain registries and registrants 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 NS5.microsoftinternetsafety.net and NS6.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.

I. With regard to the domain registries and registrars located outside of the United States, the Court respectfully requests, but does not order, that they take the same or substantially similar actions so as to neutralize the threat posed by the Citadel botnet to the citizens and financial institutions of all countries, including their own. Defendants, their representatives and persons who are in active concert or participation with them are ordered to consent to whatever actions are necessary for non-United States registries, registrars, registrants and hosts to effectuate this request.

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 in the possession of data centers operated by Linode LLC/Linode VPS Hosting and Network Operations Center, Inc./BurstNET Technologies, Inc., all pursuant to 15 U.S.C. §1116(d), shall be seized:

A. The seizure at the foregoing data centers and hosting providers shall take place on or about 9:30 a.m. Eastern Daylight Time on June 5, and no later than seven (7) days after the date of issue of this order. The seizure may continue from day to day, for a period not to exceed two (2) days, until all items have been seized. The seizure shall be made by the Federal Bureau of Investigation and/or the United States Marshals Service. The Federal Bureau of Investigation and/or the United States Marshals Service in the judicial districts where the foregoing data centers and hosting providers are located are directed to coordinate with each other and with Microsoft and its attorneys in order to carry out this Order such that disablement and/or seizure

of Defendants' materials on such servers is effected simultaneously, to ensure that Defendants are unable to operate the botnet during the pendency of this case. In order to facilitate such coordination, the United States Marshals offices in the relevant jurisdictions are set forth, as follows:

a. District of New Jersey
U.S. Marshal: Juan Mattos Jr.
U.S. Courthouse
50 Walnut Street
Newark, NJ 07102
(973) 645-2404

b. Middle District of Pennsylvania
U.S. Marshal: Martin J. Pane
Federal Building
Washington Avenue & Linden Street, Room 231
Scranton, PA 18501
(570) 346-7277

B. The Agents of the Federal Bureau of Investigation and/or the United States Marshals and their deputies shall be accompanied by Microsoft's attorneys and forensic experts at the foregoing described seizure, to assist with identifying, inventorying, taking possession of and isolating Defendants' computer resources, command and control software and other software components that are seized. The Agents of the Federal Bureau of Investigation and/or the United States Marshals shall, if necessary to isolate Defendants' malicious activity, seize Defendants' computers, servers, electronic data storage devices or media associated with Defendants' IP addresses at the hosting companies set forth above, or a live image of Defendants' data and information on said computers, servers, electronic data storage devices or media, as reasonably determined by the Agents of the Federal Bureau of Investigation, U.S. Marshals Service, and Microsoft's forensic experts and/or attorneys. Up

to four hours of Internet traffic to and from Defendants' servers associated with the IP addresses at the hosting companies set forth above shall be preserved, before disconnecting those computers from the Internet.

C. Stroz Friedberg, 1925 Century Park East, Suite 1350, Los Angeles, CA 90067, will act as substitute custodian of any and all data and properties seized and evidence preserved pursuant to this Order and shall hold harmless the Federal Bureau of Investigation and the United States Marshals Service, arising from any acts, incidents, or occurrences in connection with the seizure and possession of the Defendants' property, including any third-party claims, and the Federal Bureau of Investigation and the United States Marshals Service shall be discharged its duties and responsibilities for safekeeping of the seized materials.

D. The Federal Bureau of Investigation Agents and/or the United States Marshals accomplishing such seizure are permitted to enter the premises of the data centers operated by Linode LLC/Linode VPS Hosting and Network Operations Center, Inc./BurstNET Technologies, Inc. in order to serve copies of this Order, carry out the terms of this Order and to verify compliance with this Order. The Federal Bureau of Investigation Agents and/or the United States Marshals shall employ reasonable means necessary to carry out the terms of this Order and to inspect the contents of or connect to any computers, servers, electronic data storage devices, media, room, closets, cabinets, vehicles, containers or desks or documents and to dismantle any equipment utilized by Defendants to carry out the activities prohibited by this Order.

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

A. 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;

B. 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 Defendants domains or malicious activities on or through the IP addresses set forth in Appendix B or that might otherwise be used to circumvent this Order;

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

D. 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.

E. 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;

F. Transfer any content and software hosted on Defendants' IP addresses listed in Appendix B that are not associated with Defendants to new IP addresses not listed in Appendix B; notify any non-party owners of such content or software of 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, (Tel: 650-614-7400), to facilitate any follow-on

action;

G. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order, including the provision of sufficient and reasonable access to offices, facilities, computer networks, computers and services, so that the Federal Bureau of Investigation, United States Marshals Service, Microsoft, and Microsoft's attorneys and/or representatives may directly supervise and confirm the implementation of this Order against Defendants;

H. With respect to the complete list of IP addresses known to have been associated with the botnets at issue, listed at Appendix B, any web hosting company responsible for such IP addresses located in the United States shall reasonably assist Microsoft to confirm whether such IP addresses are supporting the botnets and, if so, take reasonable remedial steps to prevent such used by Defendants.

I. With regard to the domain registries and registrars located outside of the United States, the Court respectfully requests, but does not order, that they take the same or substantially similar actions so as to neutralize the threat posed by the Citadel botnet to the citizens and financial institutions of all countries, including their own. Defendants, their representatives and persons who are in active concert or participation with them are ordered to consent to whatever actions are necessary for non-United States registries, registrars, registrants and hosts to effectuate this request.

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 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; (2) by personal delivery upon Defendants who provided contact information in the U.S.; (3) by personal delivery through the Hague Convention on Service Abroad upon Defendants who provided contact information outside the U.S.; and (4) by publishing notice to Defendants on a publicly available Internet website.

IT IS FURTHER ORDERED, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before this Court on June 10th, 2013 at 10:00 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 $300,000 to be paid into the Court registry.

IT IS FURTHER ORDERED that, to fully neutralize the Citadel botnet malicious software that has taken control of Microsoft's property, including its Windows operating system and Internet Explorer browser, and associated files, to return control of that property to Microsoft, to end the irreparable harm to Microsoft and its customers, to abate the nuisance caused by Defendants' conduct, and to notify customers of acts they may take to permanently remove the Citadel malicious code from those computers, consistent with the terms of Microsoft's license to its Windows operating system, Microsoft shall be permitted to do the following:

1. Through Microsoft's control over the domains and IP addresses listed in Appendices A and B granted elsewhere in this Order, to cause all Citadel-infected end-user computers attempting to connect to any Citadel Command

and Control server to instead connect to one or more servers under the control of Microsoft ("the Microsoft Curative Servers");

2. For a period of two weeks or more from the date of execution of this Order, to stage on the Microsoft Curative Server a first curative configuration file (the "First Curative Configuration File") that is known to be requested by the Citadel botnet malicious software running on end-user computers, such that upon connecting to the Microsoft Curative Server, the Citadel botnet malicious software shall download, decrypt, and thereafter follow the instructions in the First Curative Configuration File;

3. To permit Microsoft to prepare the First Curative Configuration File such that it (a) stops the harmful acts of the Citadel botnet malicious software; (b) permits the infected computer to connect to antivirus websites from which assistance and tools may be obtained for removing the Citadel infection from the computer, and which are currently blocked by the Citadel botnet software; and (c) keeps the Citadel malicious software on the computer from communicating with any known Citadel Command and Control servers, and instead causes it to communicate with the Microsoft Curative Servers.

4. Beginning no sooner than two weeks from the date of execution of this Order, to permit Microsoft to stage on the Microsoft Curative Server a second curative configuration file (the "Second Curative File") that is known to be requested by the Citadel malicious software;

5. To permit Microsoft to prepare the Second Curative Configuration File such that, when an end-user of an infected computer attempts to connect to any

website on the Internet other than an antivirus website, through Internet Explorer, Google Chrome, or Mozilla Firefox web browsers, a notice (the "Curative Notice"), will be displayed to the user through their browser, and that such notice shall be displayed in the user's browser for approximately twenty minutes, during which time the user will be able only to browse to the Microsoft Curative Servers or to an antivirus website;

6. To permit Microsoft, should it be necessary and prudent in Microsoft's estimation to promote further disinfection of computers currently infected with Citadel, to alternate staging of the First and Second Curative Configuration files on the Curative Servers such that the Curative Notice shall be displayed to the users of computers infected with Citadel botnet malicious software for up to one twenty minute period every five hours for one twenty-four hour period once per week, until such time as Microsoft deems it no longer necessary to prompt the owners of such infected end-user computers to take the steps necessary to cleanse them of the Citadel botnet infection.

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. (Eastern Standard Time) on the appropriate dates listed in this paragraph.

IT IS SO ORDERED

Entered this 29th day of May, 2013.

United States District Judge