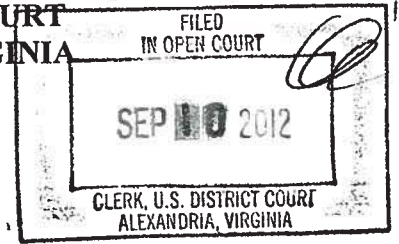


IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division



MICROSOFT CORPORATION, a)
Washington corporation,)
Plaintiff,)
v.)
Peng Yong, an individual;)
Changzhou Bei Te Kang Mu Software)
Technology Co., Ltd., d/b/a Bitcomm, Ltd;)
John Does 1-3)
Defendants.)

Civil Action No. 1:12-cv-1004 GBL
IDD

FILED UNDER SEAL

**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); and the common law of (2) trespass to chattels, (3) unjust enrichment, (4) conversion, and (5) 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 which relief may be granted against Defendants under the Computer Fraud and Abuse Act (18 U.S.C. § 1030) and the common law of 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),

51

and the common law of 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) and the common law of 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 laws through one or more of the following:

- a. intentionally and knowingly accessing and sending malicious code to the protected computers and operating systems of Microsoft and its customers without authorization, in order to infect those computers and make them part of the Nitol botnet, and intending to cause damage and benefiting therefrom;
- b. sending malicious code to configure, deploy and operate a botnet;
- c. delivering malicious code; and
- d. negligently engaging in such acts and permitting, enabling and encouraging other defendants to participate in illegal acts harmful to Microsoft, Microsoft's customers, and the general public.

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 Internet domains at issue in Microsoft's TRO

Motion and other discoverable evidence of Defendants' misconduct available through such 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 the following:

- a. Defendants have engaged in activities that directly violate United States law and harm Microsoft, its customers and the public;
- b. Defendants have continued their unlawful and/or negligent 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 Internet domains at issue in Microsoft's TRO Motion and the harmful and malicious code disseminated through these Internet domains;
- d. Defendants are likely to warn its associates engaged in such activities if informed of Microsoft's action; and
- e. Defendants have negligently allowed other defendants to use their business and resources for illegal activities.

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 intentionally illegal and/or negligent activity using the 3322.org domain that is maintained by the top level domain registry, the Public Interest Registry ("PIR"), located in Reston, Virginia.

8. There is good cause to believe that to immediately halt the injury caused by Defendants, PIR and its services provider, Afilias USA, Inc. ("Afilias") must be ordered, at 2:00

p.m. Eastern Daylight Time on September 11, 2012 or such other date and time as may be requested by Microsoft within three days of this Order:

- a. To immediately, on all authoritative name servers for the .ORG top level domain, change the Domain Name System authoritative name servers for 3322.org to “ns3.microsoftinternetsafety.net” and “ns4.microsoftinternetsafety.net,” and remove all other authoritative name servers for 3322.org, and/or change the IP address associated with 3322.org to 157.56.78.93 and/or 157.56.78.73. PIR and/or Afiliias shall reasonably cooperate with Microsoft to implement this order through one or more of the foregoing changes, as may be necessary to effectuate the terms of this order, and
- b. To immediately take all steps required to propagate the foregoing change to the Domain Name System to all parts of the Domain Name System necessary to effect this change; and
- c. To take all necessary steps to ensure that the foregoing changes remain in effect for the duration of this 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 and 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 as agreed to by Defendants in their domain name registration agreements; and

(3) publishing notice on a publically available Internet website.

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 Nitol botnet, sending malicious code to configure, deploy and operate a botnet; to infect end-user computers with other malware; or to engage in any illegal scheme to infect and control end-user computers for illegal purposes.

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 Nitol botnet or other malware-related activity, including but not limited to the command and control software hosted at and operating through the IP addresses and 3322.org sub-domains set forth herein and through any other component or element of the botnet or other malware scheme in any location.

IT IS FURTHER ORDERED that the PIR and Afiliis must:

- a. Immediately, on all authoritative name servers for the .ORG top level domain, change the Domain Name System authoritative name servers for 3322.org to "ns3.microsoftinternetsafety.net" and "ns4.microsoftinternetsafety.net," and remove all other authoritative name servers for 3322.org, and/or change the IP address associated with 3322.org to 157.56.78.93 and/or 157.56.78.73. PIR and/or Afiliis shall reasonably cooperate with Microsoft to implement this order through one or more of the foregoing changes, as may be necessary to effectuate the terms of this order, and
- b. Immediately take all steps required to propagate the foregoing change to the Domain Name System to all parts of the Domain Name System necessary to effect this change; and

- c. Take all necessary steps to ensure that the foregoing changes remain in effect for the duration of this order.
- 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 necessary to propagate the changes ordered herein to all parts of the Domain Name System;
- e. Shall save all communications to or from Defendants or Defendants' Representatives and/or related to the domains and sub-domains set forth in Appendix A;
- f. 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 authoritative name server set up and managed by Microsoft to respond to requests for the IP addresses of the sub-domains of 3322.org may respond to requests for the IP address of any domain listed in Appendix A or later determined to be associated with malware activity either by 1) giving no reply; or 2) replying with the address of a special Microsoft "sink-hole" computer, which, when contacted, shall log the date and time of the request, the IP address and related information from the requesting computer but otherwise not respond to the 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 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,

