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

MICROSOFT CORPORATION, a
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-27, CONTROLLING A
COMPUTER BOTNET THEREBY
INJURING MICROSOFT AND ITS
CUSTOMERS

Defendants.

Civil Action No: 1:10cv1056 (LMB/JFA)

BRIEF IN SUPPORT OF MICROSOFT'S REQUEST FOR ENTRY OF DEFAULT AND MOTION FOR DEFAULT JUDGMENT

Plaintiff Microsoft Corporation ("Microsoft") respectfully requests that the Court enter default and grant default judgment against Defendants who unlawfully registered and controlled 276 Internet domains that they configured to deploy and propagate the harmful Waledac botnet. This particular botnet has infected hundreds of thousands of Internet users' computers and generated hundreds of millions of harmful and unsolicited spam e-mail messages. The entry of default and a default judgment is warranted here. Microsoft served Defendants with its Complaint and Summons and related materials through the Court-ordered methods pursuant to Fed. R. Civ. P. 4(f)(3) that were reasonably calculated to provide Defendants with notice of these proceedings. Evidence exists indicating that Defendants ("Non-Responsive Defendants") did receive notice and were aware of these proceedings, and despite receiving this notice have not appeared in this action.

The Non-Responsive Defendants came to control most of the botnet domains by registering them with four internet domain registrars in China and, in one instance, took control of a domain unbeknownst to the owner. When they registered the botnet domains with the Chinese registrars, the Non-Responsive Defendants – pursuant to registrar-registrant agreements – provided names, email addresses, physical addresses and fax numbers to enable communications relating to the domains. In fact, the Non-Responsive Defendants agreed to receive, *inter alia*, notice of termination of their domains through these means.

When issuing the *Ex Parte* Temporary Restraining Order ("*Ex Parte* TRO") and the Preliminary Injunction, the Court acknowledged that the Non-Responsive Defendants had likely provided the registrars with false names and physical addresses. As such, the Court authorized service of the Complaint by alternative means pursuant to Rule 4(f)(3). (*See* D.I. 13) The Court approved four alternative means of service, including service by publication and email, that would satisfy the requirements of Due Process and were reasonably calculated to notify Non-Responsive Defendants of this action. Microsoft used these methods of service to notify Non-Responsive Defendants of this action. None of the Non-Responsive Defendants, however, have answered or otherwise responded in the months since they were notified of this action.

Accordingly, Microsoft is entitled to an entry of default and default judgment against the Non-Responsive Defendants under Fed. R. Civ. P. 55(a) and 55(b)(2). Microsoft seeks an injunction prohibiting the Non-Responsive Defendants from participating in the operation or propagation of the Waledac botnet through the 276 domains or otherwise, and transferring control to Microsoft of the 276 domains listed in the proposed order submitted herewith, so that the domains cannot be used to resuscitate the Waledac botnet.

I. STATEMENT OF FACTS

A. Procedural History

Microsoft brought suit on February 22, 2010, alleging that Defendants configured, deployed and controlled the "Waledac" computer botnet and operated hundreds of internet domains used to control it. (D.I. 1) Microsoft alleged in its Complaint that the pernicious effects of the botnet caused and continued to cause irreparable injury to Microsoft, its customers and the public, and stated claims under: (1) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) the CAN-SPAM Act, 15 U.S.C. §7704; (3) the Electronic Communications Privacy Act, 18 U.S.C. § 2701; (4) the False Designation of Origin under the Lanham Act, 15 U.S.C. §1125(a); (5) the Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c); (6) common law trespass to chattels; (7) unjust enrichment; and (8) conversion.

Microsoft simultaneously applied *ex parte* for an Emergency Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction to disable the 276 internet domains through which the Defendants controlled the botnet. (D.I. 4-5, 14) The Court issued an *Ex Parte* Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction on February 22, 2010 (D.I. 13, 27) On March 10, 2010, the Court issued a Preliminary Injunction disabling the 276 internet domains. (D.I. 38)

When it issued the *Ex Parte* TRO, the Court found good cause to permit service of Microsoft's Complaint and the related materials by alternative means pursuant to Rule 4(f)(3) and concluded the following means of service were authorized by law, satisfied Due Process, and were reasonably calculated to notify Defendants of this action: (1) 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 in China; (3) transmission by e-mail, facsimile and mail to the contact information Defendants provided to their respective domain name registrars and as agreed to by Defendants in their domain name registration agreements; and (4) publication of a notice of these proceedings on a publicly available Internet website.

B. Microsoft's Service of the Complaint on the Non-Responsive Defendants

Immediately after the Court entered its February 22, 2010 *Ex Parte* TRO, Microsoft undertook extraordinary efforts to serve Defendants with the Complaint, using the Court-ordered methods of service (*See* D.I. 13).

1. Notice And Service by Publication

On February 24, 2010, Microsoft provided notice and service of the Complaint, Summons and related materials in English and Chinese through the publicly available website www.noticeofpleadings.com. Microsoft has updated the website throughout this case. The Court's orders and notice regarding this action have also been widely reported in international media publications, including news media in China. (D.I. 32-2 at ¶¶ 15-22.) The reporting and publication of this action in China and throughout the world has been continuous. (Ramsey Decl, Ex. 11 (filed herewith).)

Non-Responsive Defendants are also very likely aware of these proceedings, as the Court's *Ex Parte* TRO and Preliminary Injunction have had a substantial negative impact on the operation of the Waledac botnet. (*Id.*, Ex. 1.) Since February, the botnet domains identified in Microsoft's Complaint have been disabled at the registry level. Disabling these domains has impeded the Waledac botnet's ability to grow and disrupted the spam email and other malicious activities the botnet spawned. (D.I. 32-1 at ¶ 2; D.I. 32-2 at ¶ 15; Ex 9.) It is virtually certain that the Non-Responsive Defendants are aware of this fact.

Given the impact of the Court's orders on the Waledac botnet and the domains supporting the botnet, the widespread publication in the media regarding these proceedings in China and elsewhere, and the publication of the pleadings through a specific Internet website, the Non-Responsive Defendants are very likely to have notice of the action and the Complaint.

There is, in fact, evidence indicating that Non-Responsive Defendants are specifically aware of the www.noticeofpleadings.com website and have actual notice. Counsel for Microsoft has monitored Internet traffic to the website between late February 2010 and the present. (Ramsey Decl., Exs. 2-5) During that four-month period, beyond the "ordinary" website traffic from a spread of IP addresses (*i.e.*, interested visitors reading the pleadings) and some obvious law enforcement visits, there have been ***thousands*** of visits from one particular IP address (212.176.17.62), associated with a company in Moscow.[1] (*Id.*, Ex. 6.) This IP address is reported as having been used in the past to carry out distributed denial-of-service attacks on a Russian language investigative journalism website. (Ramsey Decl., Ex. 7.)

Moreover, this recent traffic to the www.noticeofpleadings.com website has not been confined to merely viewing pages on the site, but has included a series of http requests designed to probe the site for potential security weaknesses. (Campana Decl., Ex. 1, ¶¶4-8; Ramsey Decl., Ex. 8) In particular, as seen in the error logs for May 2010, a number of requests have been made to the website that attempt to locate files that do not exist on the server hosting the website (and thus result in the reported errors). Among the requested files are "admin_login.asp," "login.asp," "errors.php" and many others. (*Id.*) Searching for such "login.asp" files or "errors.php" files are common first steps in carrying out website compromise techniques called "SQL Injection" or "PHP Remote File Injection." (*See* Campana Decl., Ex. 1, ¶¶4, 6; Ramsey Decl., Exs. 9, 10). Similarly, a visitor to the site was probing directories where active files that could be compromised might be located. (Campana Decl., ¶8) This is strong evidence that the Non-Responsive Defendants are not only aware of the lawsuit and the Complaint, but have deliberately accessed the www.noticeofpleadings.com website, are aware of its contents, are

[1] Counsel for Microsoft has reached out to the company controlling this IP address and is informed by technical staff at the company that it is believed that a computer associated with this IP address has been compromised and is being used to proxy communications to the www.noticeofpleadings.com website from another, unidentified computer (there are likely multiple layers of such proxy computers). (Ramsey Decl., ¶ 9)

aware of the results of the activities in this case and are attempting to retaliate.

Defendants are most likely to be attempting to carry out these activities at www.noticeofpleadings.com because their botnet has been seriously disrupted by this action and they are motivated to retaliate. Further, aggressively reaching out in this way is consistent with the prior actions of individuals associated with the Waledac botnet. Microsoft has learned that the operators of the botnet reached out aggressively in response to investigation of the botnet. Specifically, after a third-party researcher engaged in activities probing the Waledac botnet, the researcher received an email from an individual identifying themselves by the name “Wale” which issued an explicit warning to the researcher to stop attempting to disrupt the botnet.[2] (Campana Decl., ¶¶ 9 and Ex. 2)

2. **Notice And Service By Email And Through the Domain Registrars**

Between February 26, 2010 and March 3, 2010, Microsoft sent emails to the email addresses identified in the registrant contact information for the Waledac botnet domains being misused by the Non-Responsive Defendants. (D.I. 32-2 at ¶¶ 23-26.) The emails provided service of the Complaint, Summons and related materials on Non-Responsive Defendants. Of the 28 email addresses associated with the botnet domains, emails providing initial notice and service were successfully sent to 18 such addresses. The recipients have not responded to the notice. The remaining 10 email addresses were not operational and resulted in error messages when emails were sent to them. Microsoft’s counsel conducted additional research but has not discovered any other information enabling further contact information associated with the domains. (D.I. 32-2 at ¶ 31.)

Further, Microsoft’s counsel in Beijing, China has contacted the Chinese domain

[2] This text string “Wale” is present in a number of the botnet domains (e.g. “expowale.com,” “topwale.com,” “waledirekt.com,” “waleprojekt,” “waleonline.com”). (Campana Decl., ¶9)

registrars through which most of the botnet domains were registered. In March, the registrars attempted to contact the registrants through the contact information available to them pursuant to the registrar-registrant agreements. To date, however, no communications from the domain registrants have been received by the registrars, Microsoft or its counsel. (D.I. 32-2 at ¶¶ 9-14; Ramsey Decl., ¶14.)

3. <u>Notice and Personal Service to Defendants Pursuant to the Hague Convention</u>

On March 1, 2010, copies of all pleadings and orders in this action were delivered to the Ministry of Justice of the People's Republic of China, pursuant to the Hague Convention. (D.I. 32-2 at ¶ 30.) Microsoft has requested that the Ministry of Justice personally serve the documents on the Non-Responsive Defendants at the physical address information associated with the registrants of the botnet domains. There is no indication that the Ministry has been able to deliver the documents, although neither was there any indication that the request for service was refused. Investigation by Microsoft's U.S. and China counsel regarding the physical addresses associated with the domains reveal that almost all the addresses are false, thus physical service is likely to be challenging in any event. (*See* D.I. 10 at ¶¶3-5; D.I. 32-2 at ¶10.)

4. <u>Notice and Service by Facsimile</u>

Between February 27, 2010 and March 1, 2010 Microsoft made several attempts to provide notice of these proceedings and serve its Complaint via the facsimile numbers associated with the botnet domains. None of the facsimile numbers provided by the Non-Responsive Defendants are in operation. (D.I. 32-2 at ¶¶ 27-29.)

II. <u>THE COURT SHOULDER ENTER A DEFAULT JUDGMENT AGAINST THE NON-RESPONSIVE DEFENDANTS</u>

Obtaining default judgment against a party is a two-step process. Under Fed. R. Civ. P. 55(a) "when a party against whom a judgment for affirmative relief is sought has failed to plead or otherwise defend, and that failure is shown by affidavit or otherwise, the clerk must enter the party's default." Once the clerk has entered the party's default, the party seeking default judgment must apply, under Fed. R. Civ. P. 55(b)(2) to the court for a default judgment.

A. **The Clerk Should Enter Default Under Fed. R. Civ. P. 55(A) Because The Non-Responsive Defendants – Having Been Served – Have Failed to Answer Or Otherwise Appear**

Between February 24, 2010 and present, Microsoft served the Complaint on the Non-Responsive Defendants using the methods ordered by the Court in its February 22, 2010 *Ex Parte* TRO under Rule 4(f)(3), including service by email and publication. These methods of service satisfy Due Process and were reasonably calculated to notify the Non-Responsive Defendants of this action. Moreover, the evidence indicates that Non-Responsive Defendants did receive actual notice of this action.

Courts have recently come to appreciate the need to resort to alternative means of serving evasive international defendants. The Ninth Circuit in *Rio Props., Inc. v. Rio Int'l Interlink*, for example, recognized that service by email is particularly warranted in cases – such as this – involving Internet-based misconduct perpetrated by international defendants, as perhaps the only method "aimed directly and instantly" at serving international e-business defendants:

> [Defendants] had neither an office nor a door; it had only a computer terminal. If any method of communication is reasonably calculated to provide [Defendant] with notice, surely it is email-the method of communication which [Defendant] utilizes and prefers. In addition, email was the only court-ordered method of service aimed directly and instantly at [Defendant] … Indeed, when faced with an international e-business scofflaw, playing hide-and-seek with the federal court, email may be the only means of effecting service of process.

Rio Props., Inc. v. Rio Int'l Interlink, 284 F.3d 1007, 1014-15 (9th Cir. 2002). Courts since *Rio Props.*, have found email service an appropriate alternative means of service on international defendants under Rule 4(f)(3). *See e.g., FMAC Loan Receivables v. Dagra*, 228 F.R.D. 531, 534

(E.D. Va. 2005) (acknowledging that courts have readily used Rule 4(f)(3) to authorize international service through non-traditional means, including email); *see also BP Prods. N. Am. Inc., v. Dagra*, 236 F.R.D. 270, 271-273 (E.D. Va. 2005); *Williams v. Adver. Sex L.L.C.*, 231 F.R.D. 483, 486 (N.D. W. Va. 2005) (asserting, "The Fourth Circuit Court of Appeals has not addressed this issue. Therefore, in the absence of any controlling authority in this circuit, the Court adopts the reasoning of the Ninth Circuit, in *Rio Properties, Inc....*"); *Williams-Sonoma, Inc. v. Friendfinder, Inc.*, 2007 U.S. Dist. LEXIS 31299, *5-6 (N.D. Cal. Dec. 6, 2007) (finding service by email consistent with the Hague Convention and warranted in cases involving misuse of Internet technology by international defendants); *MPS IP Servs. v. Modis Communs., Inc.*, 2006 U.S. Dist. LEXIS 34473, *3 (M.D. Fla. May 30, 2006).

Pursuant to the Court's *Ex Parte* TRO, between February 26, 2010 and March 3, 2010, Microsoft sent a series of emails containing the Complaint, summons and the other documents related to this proceeding to the email addresses associated with the botnet domains registered by the Non-Responsive Defendants. Emails sent to 18 of the email addresses were successfully delivered, but Microsoft received no responses, nor did any of the China based registrars through which the domains were registered. Non-Responsive Defendants have therefore been served with the Complaint by email, but have failed to respond.

The Court also ordered service by publication of the Complaint and all pleadings on www.noticeofpleadings.com. Federal Courts routinely authorize service of international defendants by publication when it is reasonable to conclude that the defendants are likely to read the media in which the notice is published. *See BP Prods. N. Am., Inc., supra*, 236 F.R.D. at 271-273 (approving notice by publication in two Pakistani newspapers circulated in the defendant's last-known location); *Smith v. Islamic Emirate of Afghanistan*, 2001 U.S. Dist. LEXIS 21712 (S.D.N.Y. Dec. 26, 2001) (approving service by publication upon Osama bin

Laden and the al-Qaeda organization); *SEC v. HGI, Inc.*, 1999 U.S. Dist. LEXIS 17441, *4-5 (S.D.N.Y. Nov. 5, 1999) (approving service by publication in a national newspaper); *Morris v. Khadr*, 415 F.Supp. 3d 1323, 1327 (D. Utah 2006) (allowing the plaintiffs to serve defendant in Toronto by publishing notice in a newspaper and posting the complaint on a website "www.september11classaction.com").

From February 24, 2010 to the present, Microsoft published the Complaint and all pleadings on www.noticeofpleadings.com, in both English and Chinese. There are, moreover, concrete indications that this site has been visited from an IP address used to carry out "denial of service" attacks and the evidence indicates that specific steps have been taken to compromise this site, since at least May 2010. From these facts, it is reasonable to infer that, since at least May, the Non-Responsive Defendants have been fully and specifically aware of the purpose of the site and its content, including the Complaint and Summons, and that they are actively attempting to compromise it.

Indeed, Non-Responsive Defendants are almost certainly aware of the action and its impact to the 276 domains at issue and the botnet in general. First, the Court's order disabling the botnet domains has been widely reported in the press, including in China, where the Non-Responsive Defendants purportedly reside according to domain registrant details. (Ramsey Decl., Ex. 11) Further, given that the botnet operations have been disrupted, Non-Responsive Defendants would be motivated to visit the www.noticeofpleadings.com website in an attempt to retaliate by compromising the site. Indeed, the evidence indicates that on a prior occasion where a third party researcher engaged in activities potentially disrupting portions of the Waledac botnet, one of the botnet controllers reached out to issue a warning to the researcher. (Campana Decl., ¶9, Ex. 2.) This all supports the conclusion that Non-Responsive Defendants are aware of the lawsuit, are specifically aware of the www.noticeofpleadings.com website containing the

Complaint and Summons and that they have visited the website. On these bases, Non-Responsive Defendants have been served the Complaint via publication at www.noticeofpleadings.com, have actual notice of the complaint, but have failed to respond.

On March 1, 2010 copies of all pleadings and orders were delivered to the Ministry of Justice of the People's Republic of China, pursuant to the Hague Convention. Microsoft requested that the Ministry of Justice personally attempt to serve the documents on the Non-Responsive Defendants at the physical address information provided by the Non-Responsive Defendants when they registered the botnet domains. The Ministry of Justice has not objected to the request, but there is not yet an indication that service by this means has been carried out.

The evidence indicates that Non-Responsive Defendants have actual notice of the action, including by email and by website publication. Moreover, Microsoft used means explicitly endorsed by the Court as satisfying the demands of Due Process and that were reasonably calculated, in light of the circumstances, to apprise the Non-Responsive Defendants of the pendency of this action. The evidence indicates that each such means of service has been effected for greater than 21 days. In particular, greater than 21 days has elapsed both from the date of actual notice by email to registrants and from the point at which the www.noticeofpleadings.com website has been made available and has been accessed by individuals believed to be the Non-Responsive Defendants.

Thus, the Complaint should be deemed served upon Non-Responsive Defendants for a period of greater than 21 days. Despite Microsoft's extraordinary efforts to serve the Non-Responsive Defendants and provide them with notice of the action, they have failed to plead or otherwise defend against the action. Therefore under Fed. R. Civ. P. 55(b) the Clerk must enter the Non-Responsive Defendants' default.

B. <u>The Court Should Exercise Its Discretion To Enter Default Judgment Against The Non-Responsive Defendants</u>

The grant of default judgment is committed to the discretion of the court. *Park Corp. v. Lexington Ins. Co.,* 812 F.2d 894, 896 (4th Cir. 1987); *EMI April Music, Inc. v. White,* 618 F. Supp. 2d 497, 506 (E.D. Va. 2009) (Davis, J.). Factors that courts have considered in granting default judgment include: the amount of money potentially involved; whether material issues of fact or issues of substantial public importance are at issue; whether the default is largely technical; whether plaintiff has been substantially prejudiced by the delay involved; whether the grounds for default are clearly established; how harsh an effect default judgment might have; or whether the default was caused by a good-faith mistake or by excusable or inexcusable neglect on the part of the defendant." *Id* (citing Wright, Miller & Kane, Federal Practice and Procedure: Civil 3d § 2685); *see also Tweedy v. RCAM Title Loans, LLC,* 611 F. Supp. 2d 603, 606 (W.D. Va. 2009). Finally, a court, in granting default judgment, must determine whether the well-pleaded allegations in the complaint support the relief sought. *Ryan v. Homecomings Fin. Network*, 253 F.3d 778, 780-781 (4th. Cir. 2001).

1. <u>The Discretionary Factors Favor The Entry of Default Judgment Against The Non-Responsive Defendants</u>

The discretionary factors evaluated by courts in this district and circuit (*see supra*) weigh in favor of entering default judgment against the Non-Responsive Defendants. First, the amount of money requested is not merely insignificant, it is non-existent; Microsoft seeks control over the offending domains, in order to secure them, and injunctive relief against the Non-Responsive Defendants.

Second, material issues of fact are not at issue – Microsoft, in its pleadings and accompanying declarations has adduced incontrovertible evidence that the domains controlled by the Non-Responsive Defendants played a role in controlling the Waledac botnet.

Third, Non-Responsive Defendants' default is not merely technical. This is not a situation where defendants have merely missed a deadline by a few days – they have failed to appear ***in any way*** in this action, despite ample notice and opportunity to do so.

Fourth, Microsoft has been substantially prejudiced by the Non-Responsive Defendants' failure to answer or otherwise appear. Microsoft has spent considerable time, money, and effort pursuing this case, effecting service upon the Defendants and securing the Waledac botnet domains, in order to prevent the irreparable injury caused to Microsoft by the botnet. Non-Responsive Defendants' failure to answer or appear has caused Microsoft to bear the foregoing costs and prolonged the uncertainty associated with the disposition of these domains.

Fifth, the grounds for default have been clearly established – Microsoft served Non-Responsive Defendants using means that satisfied Due Process and were reasonably calculated to notify them of the action, but the Non-Responsive Defendants failed to answer or otherwise respond within the required 21 days.

Sixth, the relief sought – a permanent injunction transferring control of the botnet domains to Microsoft – is not harsh. The domains were not being used by the Non-Responsive Defendants or any other party for any legitimate purpose. Moreover, under the *Ex Parte* TRO entered by the Court on February 24, 2010, the botnet domains were locked at the registry level, which prevented the Non-Responsive Defendants from using, configuring or controlling their domains. Over the months during which they were deprived of the use of their domains, none of the Non-Responsive Defendants registered any sort of complaint with the registrars, Verisign, or Microsoft, underscoring the conclusion that permanently transferring the domains to Microsoft is not likely to impair any legitimate interest the Non-Responsive Defendants have in the botnet domains.

Indeed, under applicable ICANN rules governing the ".com" domains at issue in this case, the domains would be subject to cancellation in any event, as the Non-Responsive Defendants have provided obviously false contact information and have failed to respond to inquiries by the registrars for over 15 days. In particular, Section 3.7.7.1 of the ICANN accreditation agreement provides that domain registrants "shall provide to Registrar accurate and reliable contact details and promptly correct and update them during the term of the Registered Name registration..." (D.I. 10 at Exs. H, I). Section 3.7.7.2 of the accreditation agreement provides that "failure to respond for over fifteen calendar days to inquiries by Registrar concerning the accuracy of contact details associated with the Registered Name Holder's registration shall constitute a material breach of the Registered Name Holder-registrar contract and be a basis for cancellation of the Registered Name registration." (*Id.*). Since at least March, the China domain registrars have attempted to contact the registrants who provided false information, but received no response. (D.I. 32-2 at ¶¶ 9-14; Ramsey Decl., ¶14.) This discretionary factor weighs in favor of entry of default judgment as well.

Finally, there is no indication that the Non-Responsive Defendants' default was in any way caused by a good-faith mistake or by neglect on their part. To the contrary, Microsoft has made extraordinary efforts to ensure that Defendants were provided notice and the evidence indicates that Defendants are actually or constructively aware of this action, but have chosen not to respond.

2. The Well-Pleaded Allegations in Microsoft's Complaint Support the Relief Sought by Microsoft

The relief Microsoft seeks through default judgment is a permanent injunction prohibiting the Non-Responsive Defendants from configuring, deploying, operating or otherwise participating in or facilitating the Waledac botnet. The only way to effectively enjoin Non-Responsive Defendants' operation and propagation of the Waledac botnet is to permanently deprive them of the botnet domains and transfer control of the domains to an entity that will ensure that they are not re-infected and revived as part of the Waledac botnet. Microsoft is a natural candidate for the entity which should control these domains: it is willing to bear the costs associated with ensuring that the domain registrations do not lapse; it has the technical expertise to ensure that the domains are not once again taken over by the Waledac botnet; it has no pecuniary interest in controlling those domains. Its only interest is in ensuring that those domains do not become part of the Waledac botnet once again.

Microsoft's complaint stated claims under: (1) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) the CAN-SPAM Act, 15 U.S.C. §7704; (3) the Electronic Communications Privacy Act, 18 U.S.C. § 2701; (4) the False Designation of Origin under the Lanham Act, 15 U.S.C. §1125(a); (5) the Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c); (6) the common law trespass to chattels; (7) unjust enrichment and (8) conversion. The complaint, motion for temporary restraining order and accompanying declarations established detailed facts and overwhelming evidence that support each of those claims. Thus, entry of default is appropriate.

C. <u>The Non-Responsive Defendants' Actions Were Sufficiently Definite To Tie Them To Microsoft's Allegations In The Complaint</u>

A defendant does not need to be identified with absolute precision for a court to enter default judgment against that defendant. Courts have often entered default judgment against defendants whose names and physical addresses were never discovered but whose actions were sufficiently definite to tie them to the claims in the complaint. In *SEC v. One or More Unknown Traders in the Common Stock of Certain Issuers*, 2009 U.S. Dist. LEXIS 92128 (E.D.N.Y. 2009), the SEC was unable to discern the true identities of unknown defendants who used online brokerage accounts to trade securities in a manner that violated sections of the Exchange Act. Despite the plaintiff's inability to identify and physically locate the defendants, the court entered default judgment finding the defendants liable for violations of the Exchange Act and permanently enjoining them from further violations. Similarly, in *Transamerica Corp. v. Moniker Online Servs., LLC.*, 2010 U.S. Dist. LEXIS 48016 (S.D. Fl. 2010), plaintiff was unable to discover the true identity of "Jan Stroh" – a fictitious individual who had used a false name and fake address in registering and using internet domain names incorporating or imitating Transamerica's federally registered service mark. Despite the plaintiff's inability to identify the true name and location of "Jan Stroh," the Court entered default judgment against Stroh for violating sections of the Lanham Act.

Microsoft has adduced considerable evidence to show that the 276 internet domains identified in this action were used to control, operate and propagate the Waledac botnet. The conclusion that these domains powered the Waledac botnet is further strengthened by the precipitous decline in the Waledac botnet's activity after Verisign – authorized by a temporary restraining order and preliminary injunction from the Court – disabled these domains.

Even though the Non-Responsive Defendants' names and physical locations are not known, their actions – particularly their connections to the botnet domains – are sufficiently definite to tie them to the operation of the Waledac botnet. Each of the Non-Responsive Defendants registered or controlled one or more of the botnet domains using the services of one or more Chinese domain registrars. The Non-Responsive Defendants supplied false names, fake addresses, and inoperative fax numbers in registering the botnet domains with the China-based registrars.[3] From these facts, it is reasonable to conclude that Defendants also controlled those domains for purposes of perpetuating the botnet.[4]

[3] The single exception to this is the botnet domain "debtbgonesite.com" – the only U.S. registered domain – which included valid registrant information and turned out to be a website that was externally compromised by the Defendants. Microsoft has worked closely with the registrant since the very beginning of the case and Microsoft has acquired that particular domain.

[4] The possibility that the China-based domains were originally registered by innocent parties unconnected to the botnet and then subsequently hijacked by the operators of the Waledac botnet is practically non-existent in light of the fact that the registrants provided false contact information when registering the domains and the fact that over the last four months, during which the domains have been disabled by Verisign, not a single China-based registrant has

The lack of any response by the Non-Responsive Defendants who registered the botnet domains, despite the clear impact to the domains and despite close coordination with the China domain registrars, further supports this conclusion. Given the role those domains played in the operation and propagation of the Waledac botnet, the inescapable conclusion is that the Non-Responsive Defendants' actions played a significant role in the operation and propagation of the Waledac botnet. Thus, the Non-Responsive Defendants' actions were sufficiently definite to tie them to the matters forming the basis of the complaint.

III. CONCLUSION

For all of the foregoing reasons, entry of default by the Non-Responsive Defendants and default judgment in favor of Microsoft is appropriate. Microsoft respectfully requests entry of default judgment against Non-Responsive Defendants, transferring ownership and control of the 276 Waledac botnet domains to Microsoft and enjoining Defendants from further operating the botnet.

complained or communicated with the Chinese registrars, Verisign or Microsoft; an innocent party, suddenly deprived of access to a domain it paid for would be likely to make inquiries.

Dated: July 12, 2010.

Respectfully submitted,

ORRICK, HERRINGTON & SUTCLIFFE LLP

/s/ Preston Burton

PRESTON BURTON (Va. State Bar No. 30221)
REBECCA L. MROZ (Va. State Bar No. 77114)
ORRICK, HERRINGTON & SUTCLIFFE LLP
Columbia Center
1152 15th Street, N.W.
Washington, D.C. 20005-1706
Telephone: (202) 339-8400
Facsimile: (202) 339-8500
pburton@orrick.com
bmroz@orrick.com

Of counsel:

GABRIEL M. RAMSEY (*pro hac vice*)
JACOB M. HEATH (*pro hac vice*)
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401
gramsey@orrick.com
jheath@orrick.com

Attorneys for Plaintiff Microsoft Corp.

CERTIFICATE OF SERVICE

I hereby certify that on this 12th day of July 2010, a true and correct copy of the foregoing pleading or paper was served using the Court's CM/ECF system.

I further certify that the following parties and third parties will receive service by publication, electronic means and/or FedEx as indicated below:

Via E-mail and Publication

John Doe Defendants 1-27
noticeofpleadings.com
wangjiayan@sohu.cn
jiangchengxian_1@sina.com
caimeihui@hichina.com.cn
youyueyou@163.com
lifengzhen@sogou.cn
ed30673637@126.com
huangjiayu@tom.com
chenyanglin@tom.cn
dinglin_156@126.com
jongchangde@126.com
meishengchang@163.com
wusong_ccc@126.com
kaokga@126.com
5484585125@qq.com
caomingjie@qq.com
563232521@qq.com
pljlkeg@126.com
bpoffer@qq.com
haieya01@126.com

Via FedEx

Stephen Paluck
14625 Southwest Glenbrook Road
Beaverton, OR 97007

eNom / Demand Media
Rick Danis
Senior Director Business and Legal Affairs
eNom / Demand Media
15801 NE 24th St.
Bellevue, WA 98008

Wild West Domains
Kelly Lewis
Deputy General Counsel
Godaddy Group / Wild West Domains
14455 N. Hayden Road
Suite 219
Scottsdale, AZ 85260

Via Hand-Delivery

VeriSign, Inc.
Thomas C. Indelicarto
Vice President & Associate General Counsel
VeriSign, Inc.
21355 Ridgetop Circle
Dulles, VA 20166

Xin Net Technology Corp.
1st Floor, 2nd Building Section A
BDA BeiGongDa Software Area
Beijing, China 100176

Xiamen Ename Network Technology Corp Ltd. d/b/a/ Ename Corp.
602 Grand Imperial Plaza
No. 820 Xiahe Road
Xiamen FuJian, China 361004

Zhong Xin Qian Kun Network Technology Co., Ltd. d/b/a/ China Springboard and Namerich
Suite 101, Building 7
Spring Garden
Haidian District
Beijing, China 100089

Beijing Innovative Linkage Technology Ltd.
20/F, Block A
SP Tower Tsinghua Science Park No. 1
Zhongguancun
Beijing, China 100084

Respectfully submitted,

/s/ Preston Burton

PRESTON BURTON
(Va. State Bar No. 30221)
REBECCA L. MROZ
(Va. State Bar No. 77114)
Attorneys for Plaintiff Microsoft Corp.
ORRICK, HERRINGTON & SUTCLIFFE LLP
Columbia Center
1152 15th Street, N.W.
Washington, D.C. 20005-1706
Telephone: (202) 339-8400
Facsimile: (202) 339-8500
pburton@orrick.com
bmroz@orrick.com