Richard A. Jacobsen (RJ5136)
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, New York 10019
Telephone: (212) 506-5000
Facsimile: (212) 506-5151

Gabriel M. Ramsey (*pro hac vice*)
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, California 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

Attorneys for Plaintiffs
MICROSOFT CORPORATION,
FS-ISAC, INC. and NATIONAL AUTOMATED
CLEARING HOUSE ASSOCIATION

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MICROSOFT CORP., FS-ISAC, INC., and NATIONAL AUTOMATED CLEARING HOUSE ASSOCIATION,

Plaintiffs

v.

JOHN DOES 1-39 D/B/A Slavik, Monstr, IOO, Nu11, nvidiag, zebra7753, lexa_Mef, gss, iceIX, Harderman, Gribodemon, Aqua, aquaSecond, it, percent, cp01, hct, xman, Pepsi, miami, miamibc, petr0vich, Mr. ICQ, Tank, tankist, Kusunagi, Noname, Lucky, Bashorg, Indep, Mask, Enx, Benny, Bentley, Denis Lubimov, MaDaGaSka, Vkontake, rfcid, parik, reronic, Daniel, bx1, Daniel Hamza, Danielbx1, jah, Jonni, jtk, D frank, duo, Admin2010, h4x0rdz, Donsft, mary.J555, susanneon, kainehabe, virus_e_2003, spanishp, sere.bro, muddem, mechan1zm, vlad.dimitrov, jheto2002, sector.exploits AND JabberZeus Crew, AND YEVHEN KULIBABA AND YURIY KONOVALENKO, CONTROLLING COMPUTER BOTNETS THEREBY INJURING PLAINTIFFS, AND THEIR CUSTOMERS AND MEMBERS,

Defendants.

Case No. 12-CV-1355 (SJ) (RLM)

MOTION FOR DEFAULT JUDGMENT AND PERMANENT INJUNCTION

Plaintiffs MICROSOFT CORP. ("Microsoft"), FINANCIAL SERVICES – INFORMATION SHARING AND ANALYSIS CENTER, INC. ("FS-ISAC"), and the NATIONAL AUTOMATED CLEARING HOUSE ASSOCIATION ("NACHA") (collectively, "Plaintiffs") respectfully move the Court to grant default judgment and issue a permanent injunction against Defendants, who operated and controlled the Zeus botnets from and through the Internet domain names identified in Appendix A to the Proposed Order, filed herewith.

The Zeus botnets are estimated to have infected more than 13 million Internet users' computers. (Complaint, Dkt. No. 1, ¶¶113, 116) Through various fraudulent techniques such as spam e-mail purporting to be from legitimate organizations, including from Plaintiffs, innocent computer users are lured to websites from which malicious botnet code is surreptitiously installed on their computers. The botnet code then makes unauthorized changes to the infected computers and operating systems to bring the computer under the control of the botnet operators. The botnet code then waits for the unsuspecting user to attempt to connect to the website any one of a number of targeted financial institutions and to log into an account, during which time the botnet code captures the user's account credentials. The botnet operators then use those credentials to steal money from the account or for other illegal purposes. (*Id*. ¶¶83-104)

Default judgment is warranted here. Plaintiffs served Defendants with their Complaint and summons and related materials through Court-ordered methods pursuant to Fed. R. Civ. P. 4(f)(3). John Does 22, 23, 24 and 36 engaged Plaintiffs, and after resolution was reached, were dismissed with prejudice. The Court deemed service as to the remaining Defendants to have been reasonably calculated to provide Defendants with notice of these proceedings. (*See* November 13, 2012 Memorandum and Order, Dkt. No. 38) The remaining Defendants, John Does 1-21, 25-35, and 37-39 (hereinafter, the "Defendants") received notice and are aware of these proceedings, but despite this, a full eight months after Plaintiffs filed suit, they still have not responded or otherwise appeared in this action. Accordingly, on November 13, 2012, the Clerk of the Court entered default against them.

(*See* Civil Docket For Case #: 1:12-cv-01335-SJ-RLM, entry of November 13, 2012, attached hereto as Exhibit 1).

Plaintiffs seek default judgment against the Defendants under Fed. R. Civ. P. 55(b)(2) and an injunction 1) prohibiting the Defendants from operating or propagating the Zeus botnets, and 2) for a period of 24 months, maintaining the botnet command and control domains in their current disabled state. Allowing the botnet command and control infrastructure to come back online sooner will allow the botnet operators to reconnect with computers that still have not been disinfected.

Both the entry of default judgment and issuance of a permanent injunction are warranted. There is no money at issue in granting a permanent injunction as Plaintiffs seek only non-monetary relief at this point. Issues of substantial public importance weigh heavily in favor of a permanent injunction as lifting the injunction on the botnet infrastructure prematurely, before a sufficient 24 month period to clean infected end-user computers, will allow the botnets to resume their fraudulent and criminal operations. There are no disputed material issues of fact; Plaintiffs adduced overwhelming evidence of Defendants fraudulent acts, which was set forth in detail in the Complaint and submitted at the time they filed the Complaint (Dkt. Nos. 1-48 – 1-64, 20, 21), and no Defendant has come forward to challenge this evidence in the Complaint, or otherwise. The default is not technical or the result of excusable negligence, and the grounds for default are clearly established, as Defendants have not responded to the Complaint in any way for eight months. Plaintiffs will be prejudiced by delay, as further discovery or progress in the case is precluded by Defendants' refusal to appear. Finally, default judgment will not have any negative effect on any legitimate interest of the Defendants; the only domains affected will be those used in the botnets' illegal operations. Moreover, to the extent that the assistance of third party domain registries is needed to effect final relief against Defendants, the Court has authority under the All Writs Act to direct such limited relief, which amounts to leaving the current preliminary injunction in place for 24 months.

Accordingly, default judgment should be granted and Plaintiffs' proposed permanent injunction should be entered.

I. STATEMENT OF FACTS

A. Procedural History

On March 19, 2012, Plaintiffs filed this suit, alleging that Defendants controlled a worldwide, illegal computer network, collectively known as the Zeus botnets, comprised of end-user computers connected to the Internet that Defendants had infected with malicious software. (Dkt. No. 1) Plaintiffs estimated that Defendants, over time, had infected over 13 million computers on the Internet, enlisting them into the Zeus botnets, through which, even in the last five years, Defendants have stolen over $100 million. (Dkt. No. 1, ¶¶113, 116) Through various fraudulent techniques such as spam e-mail purporting to be from legitimate organizations, including from Plaintiffs, innocent computer users are lured to websites from which malicious botnet code is surreptitiously installed on their computers. The botnet code then makes unauthorized changes to the infected computers and operating systems to bring the computer under the control of the botnet operators. The botnet code then waits for the unsuspecting user to attempt to connect to the website any one of a number of targeted financial institutions and to log into an account, during which time the botnet code captures the user's account credentials. The botnet operators then use those credentials to steal money from the account or for other illegal purposes. (*Id.* ¶¶83-104)

Plaintiffs alleged that these acts violated 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); trademark infringement under the Lanham Act (15 U.S.C. § 1114), false designation of origin under the Lanham Act (15 U.S.C. § 1125(a)); trademark dilution under the Lanham Act (15 U.S.C. § 1125(c)); the Racketeer Influence and Corrupt Organizations Act (18 U.S.C. § 1962(c)); and the common law of unjust enrichment, trespass to chattels, and conversion. (*Id.* ¶¶114-202) Plaintiffs sought injunctive and other equitable relief against Defendants for their

creation, control, maintenance, and ongoing use of the Zeus botnets, which had caused irreparable injury to Plaintiffs, Plaintiffs' customers and members, and the general public. (*Id.* pp. 40-41) Simultaneously with the filing of the Complaint, Plaintiffs applied *ex parte* for a Temporary Restraining Order, Seizure Order, and Order to Show Cause re Preliminary Injunction. (Dkt. Nos. 1-65 – 1-69) The aim of this was to disable and seize the Zeus botnets' command and control server software, operating from and through the domain names at issue in the case.

On March 19, 2012, the Court issued an *Ex Parte* Temporary Restraining Order, Seizure Order and Order to Show Cause Re Preliminary Injunction ("the TRO"). (Dkt. No. 13) On March 23, 2012, Plaintiffs executed the TRO, disabling the targeted Zeus botnet infrastructure. On March 29, 2012, the Court issued a Preliminary Injunction disabling, during the pendency of this action, the domains through which the Defendants operated and controlled the Zeus botnets. (Dkt. No. 22)

When it issued the Preliminary Injunction, the Court found good cause to permit service of Plaintiffs' Complaint and related materials by alternative means pursuant to Rule 4(f)(3). (*Id*) Plaintiffs subsequently pursued discovery, to obtain further contact and identifying information regarding Defendants. (*See* Dkt. No. 29) Plaintiffs carried out service of process to such contact information and through the means authorized by the Court. Subsequently, Plaintiffs were able to name two of the Defendants, Yevhen Kulibaba (John Doe 22) and Yuriy Konovalenko (John Does 23, 24). On the same date, Plaintiffs informed the Court that they had resolved the matter with and as to John Doe 36, and concurrently filed a notice of dismissal with prejudice. (Dkt. No. 30) On August 31,2012, Plaintiffs filed a notice of voluntary dismissal against Kulibaba and Konovalenko (Dkt. No. 34), and on September 13, 2012, the Court ordered their dismissal. (Dkt. No. 35)

Meanwhile, despite being served the complaint, summons and other pleadings in the action over the course of many months, the remaining Defendants (John Does 1-21, 25-35, 37-39) have not responded to the complaint or appeared in the action. Accordingly, on

November 8, 2012, the Court ordered the Clerk to enter a notation of default against them (Dkt. No. 38), and the Clerk of the Court entered that notation on November 13, 2012.

B. Enjoining Defendants' Illegal Activities And Access To The Botnet Domain Names For A Period Of Twenty Four Months Will Prevent The Harm Caused By The Botnets

The Internet domain names at issue in this case, as set forth in Appendix A of the proposed order submitted with this motion, comprise the now-disabled infrastructure that Defendants used to control the Zeus botnets. (*See* Dkt. No. 1, p. 1 (Introduction)) Plaintiffs set forth detailed evidence establishing this fact in the Complaint and in connection with Plaintiffs' motion for the TRO. (*See* Dkt. Nos. 1.47-1.65) All such factual material is incorporated by reference, in support of this motion.

The permanent injunction sought by Plaintiffs directs that the Defendants cease their malicious conduct, and directs that the domains constituting the crucial infrastructure of the Zeus botnets remain offline and disabled for an additional period of 24 months. This will ensure that the operators of the Zeus botnets will not be able to control or operate the botnets for malicious purposes. Keeping these domains offline for 24 months will provide sufficient time for the installed base of infected computers to be cleaned, through Microsoft's partnering with relevant Internet service providers providing connectivity for such computers. The result will be that, after such period, the network of infected computers will be dismantled and the domains will, at that point, no longer be a threat.

II. THE COURT SHOULD ENTER DEFAULT JUDGMENT AND A PERMANENT INJUNCTION AGAINST DEFENDANTS

The law provides that obtaining default judgment against a party is a two-step process. Under Fed. R. Civ. P. 55(a) "[w]hen 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. The Clerk has already entered default

against the Defendants. Entry of a default judgment and permanent injunction against Defendants is now appropriate.

A. The Court Should Exercise Its Discretion To Enter Default Judgment And Permanent Injunction Against The Non-Responsive Defendants

The grant of default judgment is committed to the discretion of the court. *Swarna v. Al-Awadi*, 622 F.3d 123, 133 (2d Cir. 2010); *Wing v. East River Chinese Restaurant*, 884 F. Supp. 663, 669 (E.D.N.Y., 1995). Courts may consider various factors in making the determination whether default judgment should be entered, including, 1) the amount of money potentially involved; 2) whether material issues of fact or issues of substantial public importance are at issue; 3) whether the default is largely technical; 4) whether plaintiff has been substantially prejudiced by the delay involved; 5) whether the grounds for default are clearly established or are in doubt; 6) how harsh an effect a default judgment might have; or 7) whether the default was caused by a good-faith mistake or by excusable or inexcusable neglect on the part of the defendant. *See Wing v. East River Chinese Restaurant*, 884 F. Supp. 663, 669 (E.D.N.Y., 1995); *Briarpatch Ltd., L.P. v. Geisler Roberdeau, Inc.*, 513 F. Supp.2d 1, 3 (S.D.N.Y., 2007) (*citing Badian v. Brandaid Communications Corp.*, No. 03 Civ. 2424 (DC), 2004 WL 1933573 *2 (S.D.N.Y., Aug. 30, 2004); 10A Wright, Miller & Kane, Federal Practice and Procedure: Civil 2d § 2685.

In this case, these factors weigh heavily in favor of granting default judgment and entering a permanent injunction against Defendants. First, the amount of money potentially involved at this point in the action is not merely negligible, it is non-existent. Plaintiffs seek only injunctive relief prohibiting Defendants from operating the Zeus botnets or engaging in any of the malicious conduct alleged in this case. Plaintiffs also seek injunctive relief directing the relevant domain registries to maintain in their current disabled and disconnected state for an additional 24 months the domains used to control and propagate the Zeus botnets, so that the botnets cannot be revived through those domains.

Second, this case presents a matter of substantial—even grave—public importance. Through operation of the Zeus botnets, Defendants have stolen financial account credentials from unsuspecting and innocent computer users and, with that information in hand, have pilfered the financial assets of those individuals, thereby severely harming Plaintiffs, financial institutions, government agencies, and the general public. (Dkt. No. 1, ¶¶86-116) Evidence indicates that, over time, Zeus botnet code has infected over 13 million computers on the Internet and that the operators of Zeus have stolen an estimated $100 million during the previous five years. (*Id*., ¶¶110, 113) Extending the protective measures put in place as part of the preliminary injunction for an additional 24 months will help ensure that the Zeus botnet operators do not quickly reconnect with the computers they had infected prior to this lawsuit and continue to defraud the owners or users of those computers.

Additionally, the possibility of a disputed issue regarding material facts is a remote one. Plaintiffs, in their detailed Complaint, pleadings and accompanying declarations have adduced incontrovertible and overwhelming evidence that the domains at issue were used to control and propagate the Zeus botnet. (*See* Dkt. Nos. 1-47 – 1-65) Despite being served, no Defendant or any other party has appeared to dispute any issue of fact or law in this case. The allegations and evidence in the detailed Complaint and otherwise in the record establishes that the Defendants' operation of the Zeus botnets violated 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. § 1114 and § 1125(a) and (c)); the Racketeer Influence and Corrupt Organizations Act (18 U.S.C. § 1962(c)); and the common law of unjust enrichment, trespass to chattels, and conversion. (*See* Dkt. No. 1, ¶¶117-205)

Third, Defendants' default is not merely technical. This is not a situation where Defendants have merely missed a deadline by a few days. Rather, Defendants have utterly failed to appear in any way in this action, despite ample notice and opportunity to do so. Plaintiffs have made extraordinary efforts over the course of many months 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. (*See, e.g.*, Dkt. No. 29)

Fourth Plaintiffs, along with the other victims of the Zeus botnets, have been prejudiced by Defendants' delay in this lawsuit, insofar as the Defendants have refused to respond to Plaintiffs' complaint in any manner whatsoever; have refused to make their true identities known to the Court or to Plaintiffs; have refused to engage in discovery or provide any manner of justification for their conduct; and have refused to assist Plaintiffs in identifying, much less in recompensing, the wholly innocent victims of their acts.

Fifth, the grounds for default are clearly established. Even eight months after Plaintiffs filed the complaint, disabled their technical infrastructure—*thousands* of domains—by order of the Court, and launched extensive efforts to identify and serve them, Defendants have made no appearance in this case and have made no response whatsoever to the Complaint. Defendants are abusers of the Internet whose personal identities and physical locations remain unknown. Extensive investigation has led to the conclusion that they most likely reside in the Russian Federation, the Ukraine, or Romania. They operate via the Internet using aliases, and given their misconduct, presumably do not wish to be identified or located, much less submit to the authority of a United States district court, despite having directed their misconduct at the Plaintiffs and victims in this district. In the face of these difficulties, Plaintiffs went to extraordinary lengths to provide notice of this lawsuit to Defendants, and certain of the original Defendants did ultimately respond to Plaintiffs' service of process, proving its sufficiency. Defendants' failure to respond clearly establishes the grounds for default judgment.

Sixth, the effect of a default judgment will not be unduly harsh. No legitimate interests will be harmed. Plaintiffs seek only a 24-month extension of the measures already protecting the public through the Courts preliminary injunction. These steps were crafted to disable the operation of the Zeus botnets while causing the least amount of burden on the third party domain registries responsible for administering those domains. Thus far, no

third-party has complained of the effect of the Court's preliminary injunction. In addition, as noted, Plaintiffs only seek a 24-month extension in the injunctive measures, not an extension of unlimited duration.

Seventh, Defendants' default is not the result of excusable neglect. Plaintiffs went to extraordinary lengths to provide notice of this lawsuit to Defendants. (*See, e.g.*, Dkt. No. 29) It is reasonable to assume that Defendants received ample notice of the action against them and have deliberately chosen not to appear, for all of the reasons set forth in the briefing and declarations in support of Plaintiffs' request for entry of default. Indeed, it is reasonable to assume that Defendants have adopted a strategy of "laying low" while this lawsuit is pending, after which period they hope to resume their illegal acts.

Given the significant evidence and authority submitted in the Complaint and otherwise in this case, a default judgment is consistent with the policy animating the Federal Rules of Civil Procedure favoring decisions on the merits. Moreover, the other discretionary factors discussed above weigh strongly in favor of entering default judgment against Defendants. Defendants, who have exploited the robust and reliable Internet hosting and domain name facilities in this country should not be able to evade judgment and continue to harm Plaintiffs and the U.S. public merely because they have been successful in using fake identities and addresses and operated the Zeus botnets from overseas.

1. Plaintiffs Have Sufficiently Plead Their Claims

Plaintiffs' Complaint sets forth in detail the legal and factual bases for the following statutory and common law claims: (1) violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030), (2) violations of the CAN-SPAM Act (15 U.S.C. § 7704), (3) violations of the Electronic Communications Privacy Act (18 U.S.C. § 2701); (4) trademark infringement under the Lanham Act (15 U.S.C. § 1114); (5) false designation of origin under the Lanham Act (15 U.S.C. § 1125(a)); (6) trademark dilution under the Lanham Act (15 U.S.C. 1125(c)), (7) violations of the Racketeer Influenced and Corrupt Organizations Act; (8) unjust enrichment;

(9) trespass to chattels / computer trespass, and (10) conversion.

a. Defendants' Computer Fraud And Abuse Act Violations

The Computer Fraud and Abuse Act ("CFAA") penalizes, *inter alia*, a party that:

- intentionally accesses a protected computer[1] without authorization, and as a result of such conduct, causes damage (18 U.S.C. § 1030(a)(5)(C)); or
- intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer (18 U.S.C. § 1030(a)(2)(C)); or
- knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer (18 U.S.C. § 1030(a)(5)(A)).

The servers of Plaintiffs and their customers are "protected computers" under the CFAA. Defendants intentionally access Microsoft's proprietary operating system and Microsoft's customers' computers, without authorization, and burden those computers by infecting them with malicious code and executing that code without consent. The Zeus Botnets intentionally access without authorization Plaintiff Microsoft's website servers (to steal users' personal information) and Microsoft's email servers (to send huge volumes of unsolicited, malicious spam email to Microsoft's customers). The Zeus Botnets intentionally access without authorization the website servers of FS-ISAC's financial institution members, in order to access financial accounts and steal funds from these institutions and their customers. Thereby, Defendants have caused damage. (Dkt. No. 1, ¶¶ 60-116, 117-123)

The Zeus Botnets' unauthorized access is precisely the type of activity the Computer Fraud and Abuse Act is designed to prevent. *See e.g. Penrose Computer Marketgroup, Inc. v. Camin*, 682 F. Supp. 2d 202 (N.D.N.Y. 2010); *Global Policy Partners, LLC v. Yessin*, 2009 U.S. Dist. LEXIS 112472, *9-13 (E.D. Va. 2009) (accessing computer using credentials that did not belong to defendant was actionable under the CFAA); *Facebook, Inc. v. Fisher*, 2009

[1] A "protected computer" is a computer "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communications in the United States." 18 U.S.C. § 1030(e)(2)(B).

U.S. Dist. LEXIS 122578 (N.D. Cal. 2009) (CFAA violation where defendants allegedly engaged in a phishing and spamming scheme that compromised the accounts of Facebook users); *Physicians Interactive v. Lathian Sys., Inc.*, 2003 U.S. Dist. LEXIS 22868, *25 (E.D. Va. 2003) (CFAA violation where the defendant hacked into a computer and stole confidential information). Accordingly, Plaintiffs have plead and established their Computer Fraud & Abuse Act claims.

b. Defendants' CAN-SPAM Act Violations

The CAN-SPAM Act prohibits, among other acts, the initiation of a transmission of a commercial electronic mail message "that contains, or is accompanied by, header information that is materially false or materially misleading." 15 U.S.C. § 7704(a)(1). Defendants, through the botnet infrastructure, send e-mails containing false "header" information (*i.e.* originating sender, IP address, etc.) making the e-mails appear to originate from addresses purporting to be associated with Microsoft, FS-ISAC's members, and NACHA, or other false addresses, thereby disguising their origin with the purpose of misleading recipients and evading detection. (Dkt. No. 1, ¶¶ 60-116, 124-135) This is precisely what CAN-SPAM prohibits. *See Yahoo! Inc. v. XYZ Cos.*, 2011 WL 6072263, * 4 (S.D.N.Y. Dec. 5, 2011) (holding that the transmission of numerous commercial emails with subject headings that misleads recipients into believing the "Lottery Fraud" emails were authorized by plaintiff and were sent through the plaintiffs servers would violate the CAN-SPAM Act). Plaintiffs have plead and established their CAN-SPAM Act claim.

c. Defendants' Electronic Communications Privacy Act Violations

The Electronic Communications Privacy Act prohibits "intentionally access[ing] without authorization a facility through which electronic communications are provided" or doing so in excess of authorization and, in doing so, obtaining, altering, or preventing authorized access to an electronic communication while it is in electronic storage. 18 U.S.C. § 2701(a). The servers of Microsoft and FS-ISAC's members are facilities through which electronic communication

services are provided. Microsoft's licensed operating systems on end-user computers, moreover, are facilities through which electronic communication services are provided. The Zeus Botnets' malicious code, installed without authorization on infected computers, searches emails and other files, intercepts user communications to and from websites of Microsoft, FS-ISAC's members and other companies, steals the contents of those communications stored on computers, and steals end-user's banking credentials and other information. Once harvested, the stolen credentials are used to steal personal information and money or to send spam email from compromised email accounts. (Dkt. No. 1, ¶¶ 60-116, 136-143) Obtaining stored electronic information in this way, without authorization, is a violation of the Electronic Communications Privacy Act. *See Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC*, 759 F. Supp. 2d 417 (S.D.N.Y. 2010) (holding that an employer's unauthorized access of an employee's personal emails stored on a third-party communication service provider' system violated the ECPA). Plaintiffs have plead and established their Electronic Communication Privacy Act claim.

d. Defendants' Lanham Act Violations

Section 1114(1) of the Lanham Act prohibits use of a reproduction, counterfeit, copy or "colorable imitation" of a registered mark in connection with the distribution of goods and services where such use is likely to cause confusion or mistake or to deceive. Defendants distribute copies of Plaintiffs' and their members' registered, famous and distinctive trademarks in fraudulent websites and spam e-mail, which deceive victims, causing them confusion and causing them to mistakenly associate Plaintiffs with this activity. The Zeus Botnet also uses Plaintiffs' and their members registered, famous and distinctive trademarks in website templates and spam templates that Defendants then use to mislead Internet users into providing their website and banking credentials). Defendants steal those credentials and use them to raid Internet users' financial accounts. Defendants' creation and use of counterfeit trademarks in connection with such severe fraud is likely to cause confusion and mistake and to deceive

consumers. (Dkt. No. 1, ¶¶ 60-116, 144-166)

This is a clear violation of the Lanham Act § 1114. *Audi AG v. Shokan Coachworks, Inc.*, 592 F. Supp. 2d 246, 279 (N.D.N.Y. 2008) (use of the plaintiffs' marks in the defendants' email addresses created a likelihood of consumer confusion); *Kuklachev v. Gelfman*, 629 F. Supp. 2d 236, 258 (E.D.N.Y. 2008) (Lanham Act § 1114 violation for infringement of trademarks where confusion was likely to result from use of plaintiffs' name and images in connection with defendants' advertisements); *Brookfield Commc'ns. v. W. Coast Entm't Corp.*, 174 F.3d 1036, 1066-1067 (9th Cir. 1999) (Lanham Act §1114 for infringement of trademark in software and website code).

The Lanham Act also prohibits use of a trademark, any false designation of origin, false designation of fact or misleading representation of fact which:

> is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person.

15 U.S.C. § 1125(a). The Zeus Botnets' misleading and false uses of trademarks—including "Microsoft," "Outlook," "Windows," "NACHA," the NACHA logo, and trademarks of FS-ISAC members causes confusion and mistake as to Plaintiffs' and their affiliation with the malicious conduct carried out by the botnet. (Dkt. No. 1, ¶¶ 86-116, 117-123) This activity is a clear violation of Lanham Act § 1125(a). *See CJ Prods. LLC v. Snuggly Plushez LLC*, 809 F. Supp. 2d 127, 147-48 (E.D.N.Y. 2011) (Lanham Act § 1125(a) violation for infringement of trademark on a website); *Brookfield Commc'ns.*, 174 F. 3d at 1066-67 (Lanham Act §1125(a) violation for infringement of trademark in software and website code); *Hotmail Corp. v. Van$ Money Pie, Inc.*, 47 U.S.P.Q.2d (BNA) 1020,1024, 1025-26 (N.D. Cal. 1998) (copying the Hotmail trademarks in "e-mail return addresses" constituted false designation of origin); *Am. Online v. IMS*, 24 F. Supp. 2d 548, 551-552 (E.D. Va. 1998) (misuse of trademark in e-mail headers violated §1125(a)).

The Lanham Act further provides that the owner of a famous, distinctive mark "shall be

entitled to an injunction against another person" who uses the mark in a way "that is likely to cause dilution by blurring or dilution by tarnishment of the famous mark. . . ." 15 U.S.C. § 1125(c). Here, Defendants' misuse of Plaintiffs' famous marks in connection with malicious conduct aimed at Plaintiffs' customers and the public dilutes the famous marks by tarnishment and by blurring consumers' associations with the marks. (Dkt. No. 1, ¶¶ 86-116, 161-166) This is another clear violation of the Lanham Act. *See e.g. Hamzik v. Zale Corp.*, 2007 U.S. Dist. LEXIS 28981 (N.D.N.Y. April 18, 2007); *Hotmail Corp.*, 47 U.S.P.Q.2d at 1024, 1025-26; (spam e-mail with purported "from" addresses including plaintiff's trademarks constituted dilution); *Am. Online*, 24 F. Supp. 2d at 552 (same).

e. Trespass to Chattels/Conversion

A trespass to chattels occurs where a defendant intentionally and without justification or consent, interferes with the use and enjoyment of personal property in the plaintiff's possession and, as a result, causes damages. *Sch. of Visual Arts v. Kuprewicz*, 3 Misc. 3d 278, 281 (2003); *Yo! Braces Orthodontics, PLLC v. Theordorou*, 2011 N.Y. Misc. LEXIS 1820, *8 (Apr. 19, 2011). Similarly, conversion occurs where a defendant makes an unauthorized assumption and exercise of the right of ownership over goods belonging to another, to the exclusion of the owner's rights. *Thyroff v. Nationwide Mut. Ins. Co.*, 8 N.Y.3d 283, 284, 288-89 (2007) (conversion applies to electronic computer records and data).

Defendants have interfered with and taken as their own Plaintiffs' resources, by installing software that interferes with (1) Microsoft's licensed Windows operating system and customer computers and (2) Microsoft's and FS-ISAC's members' website servers, to steal information and money and send vast quantities of spam e-mail. (Dkt. No. 1, ¶¶ 60-116, 182-193) These activities injure the value of Plaintiffs' property and constitute a trespass and conversion. *See Thyroff*, 8 N.Y.3d at 288-89 (conversion of intangible property); *Sch. of Visual. Arts*, 3 Misc. 3d at 282 (sending unsolicited bulk email states claim for trespass to chattels; processing power and disk space adversely affected); *see also Kremen v. Cohen*, 337

F.3d 1024, 1034 (9th Cir. 2003) (hacking into computer system and injuring data supports a conversion claim); *Physicians Interactive v. Lathian Sys.*, 2003 U.S. Dist. LEXIS 22868, at *25, 31 (E.D. Va. 2003) (conversion/trespass where defendant hacked computers and obtained proprietary information).

f. Unjust Enrichment

The elements of a claim of unjust enrichment are that a (1) defendant benefitted, (2) at plaintiff's expense, and (3) equity and good conscience require restitution. *Beth Israel Med. Ctr. v. Horizon Blue Cross and Blue Shield*, 448 F.3d 573, 586 (2d Cir. 2008). Defendants controlling the Zeus Botnets have benefited from Plaintiffs' trademarks, brand names, and goodwill by, among other things, using Plaintiffs' trademarks, brand names and goodwill to further Defendants' banking fraud on Plaintiffs' customers and members. (Dkt. No. 1, ¶¶ 60-116, 194-205)

Defendants have specifically taken, without authorization, the benefit of Microsoft's and FS-ISAC's members' computers in order to steal information and money and send spam email. In each instance, Defendants have profited from their unlawful activity, reaping at least $100 million dollars in stolen money and information. Thus, it is certainly inequitable for Defendants controlling the Zeus Botnets to retain these benefits. Accordingly, Plaintiffs have plead and established their unjust enrichment claim.

g. Defendants' Racketeer Influenced and Corrupt Organizations Act (RICO) Violations

The Racketeer Influenced and Corrupt Organizations Act ("RICO") prohibits "any person employed by or associated with any enterprise engaged in, or the activities of which affect, interstate or foreign commerce to conduct or participate, directly or indirectly, in the conduct of such enterprise's affairs through a pattern of racketeering activity." 18 U.S.C. § 1962(c). RICO also makes it unlawful "for any person to conspire to violate" that provision, regardless of whether that conspiracy ultimately comes to fruition. 18 U.S.C. §1962(d). "Any person injured in his business or property by reason of a violation of" either of these provisions is entitled to

recovery, 18 U.S.C. § 1964(c), and this court has "jurisdiction to prevent and restrain" such violations "by issuing appropriate orders." 18 U.S.C. 1964(a). *See also United States v. Carson*, 52 F.3d 1173, 1181-82 (2d Cir. 1995) ("the jurisdictional powers in § 1964(a) serve the goal of foreclosing future violations," and "the equitable relief under RICO is intended to be broad enough to do all that is necessary."); *United States v. Sasso*, 215 F.3d 283, 290 (2d Cir. 2000) (same); *Trane Co. v. O'Connor Sec.*, 718 F.2d 26, 29 (2d Cir. 1983) (injunction proper under RICO where plaintiff establishes "a likelihood of irreparable harm").

Defendants in this case have formed and associated with such an enterprise affecting foreign and interstate commerce and have engaged in an unlawful pattern of racketeering activity involving thousands of predicate acts of "access device" fraud, 18 U.S.C. § 1029, as well as wire fraud, 18 U.S.C. § 1343 and bank fraud, 18 U.S.C. § 1344. (Dkt. No. 1, ¶¶ 5-116, 167-181)

(1) <u>The Zeus Enterprise</u>

An associated in fact enterprise consists of "a group of persons associated together for a common purpose of engaging in a course of conduct" and "is proved by evidence of an ongoing organization, formal or informal, and by evidence that the various associates function as a continuing unit." *Boyle v. United States*, 556 U.S. 938, 945 (2009). An enterprise requires "at least three structural features: a purpose, relationships among those associated with the enterprise, and longevity sufficient to permit these associates to pursue the enterprise's purpose." (*Id.*)

The Zeus Enterprise has existed since at least October of 2010, when John Doe 1 and John Doe 3 merged their botnet operations into a single, consolidated global credential stealing botnet. (Dkt. No. 1, ¶¶ 71-82) John Doe 2 joined the conspiracy and began participating in the Zeus Enterprise prior to fall of 2011, when John Doe 2's Zeus variant, "Ice-IX," was released. (*Id.*) John Does 4-39 joined and began participating in the Zeus Enterprise at various times thereafter. (*Id.*) *See also United States v. Eppolito*, 543 F.3d 25, 49 (2d Cir. 2008) (an enterprise "may continue to exist even though it undergoes changes in membership."). The Zeus Enterprise

has continuously and effectively carried out its purpose of developing and operating global credential stealing botnets ever since, and will continue to do so absent the relief Plaintiffs request. (*Id.*)

The consolidation of the botnet code and Defendants' interrelated roles in the operation of the Zeus Botnets, in furtherance of common financial interests, demonstrate the purpose of the Zeus Enterprise and the relationship between the Defendants. *Boyle*, 556 U.S. at 945 (relationship and common interest may be inferred from "evidence used to prove the pattern of racketeering activity"); *Eppolito*, 543 U.S. at 50 ("evidence of prior uncharged crimes. . . may be relevant. . . to prove the existence, organization and nature of the RICO enterprise, and a pattern of racketeering activity by each defendant."). The relationship between Defendants may also be inferred by the Defendants' development and/or purchasing of the Zeus botnet code and their use of the Zeus botnet system to steal and exploit customer credentials. (Dkt. No. 1, ¶¶ 71-82)

(2) Defendants' Pattern of Racketeering Activity

A pattern of racketeering activity "requires at least two acts of racketeering activity, one of which occurred after [October 15, 1970,] and the last of which occurred within ten years. . . after the commission of a prior act of racketeering activity." *H.J. Inc. v. Northwestern Bell Tel. Co.*, 492 U.S. 229, 237 (1989). A threat of continuing activity "is generally presumed when the enterprise's business is primarily or inherently unlawful." *Spool v. World Child Int'l Adoption Agency*, 520 F.3d 178, 185 (2d Cir. 2008). Defendants have conspired to, and have, conducted and participated in the operations of the Zeus Enterprise through a continuous pattern of racketeering activity. Each predicate act is related and in furtherance of the common unlawful purpose shared by the members of the Zeus Enterprise. These acts are continuing and will continue unless and until this Court enters the requested permanent injunction. (Dkt. No. 1, ¶¶ 5-116)

Defendants acts of racketeering activity include access device fraud, in violation of 18 U.S.C. § 1029. Whoever "knowingly and with intent to defraud traffics in or uses one or more

unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that that period," is guilty of violating 18 U.S.C. § 1029 "if the offense affects interstate or foreign commerce." 18 U.S.C. §1029(a)(2). An "access device" includes "any. . . code, account number, electronic serial number, mobile identification number [or] personal identification number. . . that can be used, alone or in conjunction with another access device, to obtain money. . . or any other thing of value, or that can be used to initiate a transfer of funds." 18 U.S.C. §1029(e)(1). An "unauthorized access device" includes "any access device that is lost, stolen. . . or obtained with intent to defraud." 18 U.S.C. §1029(e)(3). Violation of this statute constitutes "racketeering activity." 18 U.S.C. §1961(1)(B).

Defendants have conspired to, and have, knowingly and with intent to defraud trafficked in thousands of unauthorized access devices in the form of stolen passwords, bank account numbers and other account login credentials through the Zeus botnet system created and operated by Defendants. (Dkt. No. 1, ¶¶ 5-116.) As set forth in detail in the Complaint, Defendants have used the Zeus botnet system to intrude upon the computers of Plaintiffs, their members and customers, and steal, intercept and obtain this access device information from thousands of individuals using falsified web pages, and have then used these fraudulently obtained unauthorized access devices to steal *millions* of dollars from these individuals' accounts, in violation of 18 U.S.C. § 1029(a)(2).[2] Each of these illegal acts were conducted using interstate and/or foreign wires, and therefore affected interstate and/or foreign commerce.[3]

(3) Microsoft's and NACHA's Injury Is a Direct Result of Defendants' Pattern of Racketeering Activity

[2] Defendants' conduct also constitutes access device fraud under 18 U.S.C. §1029(a)(3) (possession of unauthorized access devices) and 18 U.S.C. §1029(a)(7) (effecting transactions with unauthorized access devices).

[3] Defendants' conduct is also "racketeering activity" in the form of bank fraud under 18 U.S.C. § 1344 (violation where one "knowingly executes, or attempts to execute, a scheme or artifice (1) to defraud a financial institution; or (2) to obtain any of the moneys, funds, credits, assets, securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations, or promises"), and wire fraud under 18 U.S.C. § 1343 (violation where one "having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire. . . communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice.").

Defendants Botnets have carried out such massive theft by infecting millions of computers running Microsoft's Windows operating system with its malicious software and flooded millions of email accounts, including hundreds of thousands of Microsoft Hotmail email accounts, with spam messages infringing Microsoft's and NACHA's trademarks, and containing links designed to infect computers with malicious software and steal credentials. As a direct result of Defendants' conduct, Microsoft and NACHA have been forced to expend resources to clean infected systems running Microsoft software, mitigate the impact to customers, and investigate the source. (Dkt. No. 1, ¶¶ 71-116) Accordingly, "there [is] a direct relationship between [the] injury and the defendant's injurious conduct" and "the RICO violation was the but-for (or transactional) cause of [the] injury." *UFCW Local 1776 v. Eli Lilly & Co.*, 620 F.3d 121, 132 (2d Cir. 2010) (citing *Holmes v. Sec. Investor Prot. Corp.*, 503 U.S. 258, 268 (1992)).[4]

2. The Permanent Injunction Sought Is Appropriate Final Relief And Necessary To Prevent The Injury Caused By The Botnets.

The record is replete with evidence that the domains at issue in this case, set forth in Appendix A of the proposed order submitted with this motion, have been used to control the Zeus botnets. Extending the measures already imposed by the Court to disable and disconnect these domains is critical to preventing the revival and renewed operation of the botnets. Therefore, relief directing the Defendants not to engage in the alleged activities, and more importantly, directing the relevant Internet service providers that the botnet domains should be kept disabled and offline for an additional 24 month period is the only way to effectively cure the harms complained of in this action. If the botnet domains are not kept offline for this period, Defendants could regain access to them and use them to revive the Zeus botnets. This would occur because currently infected computers are programmed by the botnet malware to attempt to communicate with the botnet operators through that infrastructure. (Dkt. No. 1, ¶¶86-107)

[4] Where the pattern of racketeering activity consists of fraud, as here, a plaintiff need not show that it relied on or was deceived by the defendant's fraud – third party reliance is sufficient. *Id.*, *quoting Bridge v. Phoenix Bond & Indem. Co.*, 533 U.S. 639, 657-58 (2008).

Issuance of the requested permanent injunction is appropriate in this case because the traditional four-factor test for granting a permanent injunction is satisfied. *See World Wide Polymers, Inc. v. Shinkong Synthetic Fibers Corp*., 694 F.3d 155, 160-161 (2d Cir., 2012) (*citing eBay Inc. v. MercExchange LLC*, 547 U.S. 388, 391 (2006)). First, Plaintiffs have suffered an irreparable injury through the unauthorized intrusion into their operating system installed on customer computers, the infringement and dilution of their trademarks by the spam messages disseminated by the Zeus botnets, the theft of customers' financial account credentials, and the pilfering of their financial assets. (*See* Dkt. No. 1, ¶¶108-116) Second, Plaintiffs' injury cannot be compensated adequately by remedies at law – monetary damages would be inadequate to compensate Plaintiffs if Defendants were able to revive the Zeus botnets. (*See id*). Third, the balance of hardships tips sharply in Plaintiffs' favor – Defendants were not using the relevant botnet domains for any legitimate purpose, but Plaintiffs would have to expend significant resources to filter and remediate the effects of increased illegal activity if the Zeus botnets were revived. (*See id.*) Finally the public interest would undoubtedly be served by ensuring that the Zeus botnets are not revived – the botnets took over end-users' computers, used them to disseminate spam that infringed, stole financial account credentials, and used that information to steal from those accounts. (*See id.*)

Moreover, the injunction has been tailored only to keep the domains offline for a limited period sufficient to achieve this relief. Accordingly, there is no risk that the injunction will impact any legitimate interest of any party. In particular, the third-party domain registries responsible for administering the botnet domains must simply keep in place for 24 months the relief already imposed. No additional steps are needed. Plaintiffs have been in communication with the registries throughout the case and they agreed to abide by the court's orders. Accordingly, the requested injunction is appropriate, as courts routinely enter permanent injunctions ordering stipulated relief. *See e.g. Federal Trade*

Commission v. Sonya Lockery, No. 302CV01722RNC, 2002 WL 32151635 (D. Conn., Oct. 4, 2002).

Federal courts also have the authority under the All-Writs Act, 28 U.S.C. 1651 to order injunctive relief directing third parties to perform actions that are necessary to ensure effective implementation of court orders. *See United States v. New York Telephone Co.*, 434 U.S. 159, 174 (1977) (third party technical assistance required to implement order against Defendants); *In re Stabile*, 436 F.Supp.2d 406, 413-14 (E.D.N.Y., 2006) ("The Act's grant of authority is plainly broad and, on its face, makes no distinctions between parties and nonparties.") (*quoting United States v. Int'l Bhd. of Teamsters*, 266 F.3d 45, 49-50 (2d Cir. 2001); *Eppley v. Mulley*, No. 1:09-cv-386-SEB-MJD, 2011 U.S. Dist. LEXIS 37094, at *8-*12 (S.D. Ind. Mar. 30, 2011) (granting permanent injunction against Defendants and directing third party internet service providers hosting or otherwise controlling websites to disable such websites, pursuant to All Writs Act). Here, the assistance of the third party registries is necessary to ensure that Defendants are unable to regain control over the botnet domains and that the permanent injunction against Defendants is effective and those parties have agreed to the requested relief. For all of these reasons, the requested injunction is appropriate.

B. Defendants' Actions Were Sufficiently Definite To Tie Them To Plaintiffs' Allegations In The Complaint

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. For example, in *SEC v. One or More Unknown Traders in the Common Stock of Certain Issuers*, No. 08-CV-1402, 2009 U.S. Dist. LEXIS 92128 (E.D.N.Y. Oct. 2, 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 Services., LLC.*, 2010 U.S. Dist. LEXIS 48016 (S.D. Fla. Apr. 7, 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.

Plaintiffs have adduced considerable evidence to show that the domain names identified in this action were used to control, operate and propagate the Zeus botnets. As detailed in Plaintiffs' Request for Certificate of Default, service of process was directed specifically at the nicknames, names and contact information specifically associated with the botnet domains. (Dkt. No. 32)

Even though the Defendants' "real" names and physical locations are not known, their actions – particularly their connections to the domains – are sufficiently definite to tie them to the operation of the Zeus botnets. Defendants leased one or more of the domains through which the botnet was controlled. They supplied false names, fake addresses, inoperative fax numbers and other false information in leasing these domains, whether they leased them directly from U.S. based Internet providers, or foreign re-sellers. Service was effected to the same contact information provided by Defendants, and there was no response. The lack of any response by Defendants to the disabling of the domains is also telling – had Defendants been conducting any legitimate activity from these domains, they would have contacted either the registrars/registries to complain about their domains being disabled. Given the role those domains played in the operation and propagation of the Zeus botnets, the inescapable conclusion is that Defendants played a significant role in the operation and

propagation of the botnets. Thus, 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 judgment in favor of Plaintiffs and a permanent injunction against Defendants is appropriate. Plaintiffs respectfully request entry of default judgment against Defendants and a permanent injunction prohibiting Defendants from engaging in the conduct underlying this case and directing that the botnet domains at issue continue to be disconnected for an additional period of 24 months.

Dated: November 28, 2012
New York, New York

Respectfully Submitted,

ORRICK, HERRINGTON & SUTCLIFFE LLP

By: s/ Gabriel M. Ramsey

Richard A. Jacobsen
51 West 52nd Street
New York, NY 10019
Tel: (212) 506-5000
Fax: (212) 506-5151
rjacobsen@orrick.com

Gabriel M. Ramsey (*pro hac vice*)
1000 Marsh Road
Menlo Park, California 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401
gramsey@orrick.com

Attorneys for Plaintiffs
Microsoft Corporation
National Automated Clearing House Association
FS-ISAC, Inc.

EXHIBIT 1

U.S. District Court
Eastern District of New York (Brooklyn)
CIVIL DOCKET FOR CASE #: 1:12-cv-01335-SJ-RLM

Microsoft Corp. et al v. John Does 1-39
Assigned to: Judge Sterling Johnson, Jr
Referred to: Magistrate Judge Roanne L. Mann
Cause: 15:1125 Trademark Infringement (Lanham Act)

Date Filed: 03/19/2012
Jury Demand: Plaintiff
Nature of Suit: 840 Trademark
Jurisdiction: Federal Question

Plaintiff

Microsoft Corp.

represented by **Gabriel M. Ramsey**
Orrick, Herrington & Sutcliffe LLP
1000 Marsh Road
Menlo Park, CA 94025
650-614-7400
Email: gramsey@orrick.com
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Jacob M. Heath
Orrick, Herrington & Sutcliffe LLP
1000 Marsh Road
Menlo Park, CA 94025
650-614-7400
Email: jheath@orrick.com
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Jeffrey L. Cox
Orrick, Herrington & Sutcliffe LLP
701 5th Avenue
Ste. 5600
Seattle, WA 98104
206-839-4300
Email: jcox@orrick.com
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Richard A. Jacobsen
Orrick, Herrington & Sutcliffe LLP
51 West 52nd Street
New York, NY 10019
212-506-5000
Fax: 212-506-5151
Email: rjacobsen@orrick.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Plaintiff

FS-ISAC, Inc. represented by **Gabriel M. Ramsey**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Jacob M. Heath
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Jeffrey L. Cox
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Richard A. Jacobsen
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Plaintiff

National Automated Clearinghouse Association represented by **Gabriel M. Ramsey**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Jacob M. Heath
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Jeffrey L. Cox
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Richard A. Jacobsen
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

V.

Defendant

John Does 1-39
controlling computer Botnets thereby

injuring plaintiffs and their customers
and members
doing business as
Slavik
doing business as
Monstr
doing business as
IOO
doing business as
Null
doing business as
nvidiag
also known as
zebra7753
doing business as
lexa_Mef
doing business as
gss
doing business as
iceIX
doing business as
Harderman
doing business as
Gribodemon
doing business as
Aqua
doing business as
aquaSecond
doing business as
it
doing business as
percent
doing business as
cp01
doing business as
hct
doing business as
xman
doing business as
Pepsi
doing business as
miami
doing business as
miamibc
doing business as
petr0vich
doing business as
Mr. ICQ
doing business as
Tank
doing business as
tankist
doing business as
Kusunagi

doing business as
Noname
doing business as
Lucky
doing business as
Bashorg
doing business as
Indep
doing business as
Mask
doing business as
Enx
doing business as
Benny
doing business as
Bentley
doing business as
Denis Lubimov
doing business as
MaDaGaSka
doing business as
Vkontake
doing business as
rfcid
doing business as
parik
doing business as
reronic
doing business as
Daniel
doing business as
bx1
doing business as
Daniel Hamza
doing business as
Danielbx1
doing business as
jah
doing business as
Jonni
doing business as
jtk
doing business as
Veggi Roma
doing business as
D frank
doing business as
duo
doing business as
Admin2010
doing business as
h4x0rdz
doing business as
Donsft

doing business as
mary.J555
doing business as
susanneon
doing business as
kainehabe
doing business as
virus_3_2003
doing business as
spaishp
doing business as
sere.bro
doing business as
muddem
doing business as
mechan1zm
doing business as
vlad.dimitrov
doing business as
jheto2002
doing business as
sector.exploits
doing business as
JabberZeus Crew

Defendant

JabberZeus Crew

Defendant

Yevhen Kulibaba
TERMINATED: 08/31/2012

Defendant

Yuriy Konovalenko
TERMINATED: 08/31/2012

Date Filed	#	Docket Text
11/13/2012		Clerk's ENTRY OF DEFAULT It appearing from the docket maintained in this action that Defendants John Does 1-21, 25-35, and 37-39 have failed to appear or otherwise defend this action, the default of Defendants John Does 1-21, 25-35,and 37-39 is hereby noted pursuant to Rule 55a of the Federal Rules of Civil Procedure. (Hamilton, Janet) (Entered: 11/13/2012)
11/13/2012	38	MEMORANDUM AND ORDER dated 11/8/12 that the Court finds that Defendants 1-21, 25-35, and 37-39 have failed to plead or otherwise defend the action and hereby directs the Clerk of the Court to enter a notation of default against them. (Ordered by Judge Sterling Johnson, Jr on 11/8/2012) (Guzzi, Roseann) (Entered: 11/13/2012)
11/07/2012		ORDER granting 37 Motion to Continue: Status Conference set for 11/8/2012 is adjourned to 11/29/2012 09:30 AM in Courtroom 6B South before Judge Sterling Johnson Jr. Ordered by Judge Sterling Johnson, Jr on

		11/7/2012. (Rodriguez, Ana) (Entered: 11/07/2012)
11/06/2012	37	Letter MOTION to Adjourn Conference by FS-ISAC, Inc., Microsoft Corp., National Automated Clearinghouse Association. (Ramsey, Gabriel) Modified on 11/7/2012 (Rodriguez, Ana). (Entered: 11/06/2012)
10/15/2012		NOTICE re the Status Conference set for 10/26/2012 is adjourned to 11/8/2012. (Rodriguez, Ana) Modified on 10/15/2012 (Rodriguez, Ana). (Entered: 10/15/2012)
10/15/2012		Notice of Hearings: Status Conference set for 10/19/2012 is adjourned to 11/8/2012 09:30 AM in Courtroom 6B South before Judge Sterling Johnson Jr. (Rodriguez, Ana) (Entered: 10/15/2012)
09/28/2012		Minute Entry for proceedings held before Judge Sterling Johnson, Jr: Case called. Status Conference held on 9/28/2012. The Court notes a decision is pending. Status Conference set for 10/19/2012 09:30 AM in Courtroom 6B South before Judge Sterling Johnson Jr. (Court Reporter Fred Guerino.) (Rodriguez, Ana) (Entered: 10/04/2012)
09/14/2012	36	MEMORANDUM in Support re 32 Request for Certificate of Default filed by Microsoft Corp.. (Attachments: # 1 Declaration of Gabriel M. Ramsey in Support of Motion for Entry of Default, # 2 Exhibit 1, # 3 Exhibit 2, # 4 Exhibit 3, # 5 Exhibit 4, # 6 Exhibit 5, # 7 Exhibit 6, # 8 Exhibit 7, # 9 Exhibit 8, # 10 Exhibit 9, # 11 Exhibit 10, # 12 Exhibit 11, # 13 Exhibit 12, # 14 Exhibit 13) (Jacobsen, Richard) (Entered: 09/14/2012)
09/13/2012	35	Order of Dismissal as to defendants' Yevhen Kulibaba and Yuriy Konovalenko with prejudice. (Ordered by Judge Sterling Johnson, Jr on 9/4/2012) (Guzzi, Roseann) (Entered: 09/13/2012)
09/06/2012		Minute Entry for proceedings held before Judge Sterling Johnson, Jr: Case called. Gabriel Ramsey appearing. Status Conference held on 9/6/2012. The Court vacates its prior ruling regarding default judgment and directs the plaintiff to brief the Court on the lawful service of anonymous, foreign defendants allegedly conducting tortious acts against Plaintiff via cyberspace. Brief due filed by 9/14/2012. Status Conference set for 9/28/2012 09:30 AM in Courtroom 6B South before Judge Sterling Johnson Jr. (Court Reporter Lisa Schmid.) (Rodriguez, Ana) (Entered: 09/07/2012)
08/31/2012	34	NOTICE of Voluntary Dismissal by FS-ISAC, Inc., Microsoft Corp. */Notice of Yevhen Kulibaba and Yuriy Konovalenko* (Jacobsen, Richard) (Entered: 08/31/2012)
08/21/2012		Notice of Hearings: Status Conference set for 9/6/2012 09:30 AM in Courtroom 6B South before Judge Sterling Johnson Jr. (Rodriguez, Ana) (Entered: 08/21/2012)
08/17/2012	33	Request for Certificate of Default by FS-ISAC, Inc., Microsoft Corp., National Automated Clearinghouse Association (Attachments: # 1 Affidavit in Support, # 2 Affidavit of Service /Proofs of Service to Various Defendants by Gabriel M. Ramsey) (Ramsey, Gabriel) (Entered: 08/17/2012)
08/02/2012	32	Request for Certificate of Default by FS-ISAC, Inc., Microsoft Corp., National Automated Clearinghouse Association (Attachments: # 1

		Declaration Of Gabriel M. Ramsey In Support, # 2 Proposed Order) (Jacobsen, Richard) (Entered: 08/02/2012)
07/31/2012		Minute Entry for proceedings held before Judge Sterling Johnson, Jr: Case called. Counsel Gabriel Ramsey appearing for plaintiff. Status Conference held on 8/1/2012. Plaintiff will move for default judgment against 37 defendants and requests and additional 90 days against the remaining two. Counsel is directed to file it motion for the Court's review. Status Conference set for 10/26/2012 09:30 AM in Courtroom 6B South before Judge Sterling Johnson Jr. (Court Reporter Holly Driscoll.) (Rodriguez, Ana) Modified on 8/2/2012 (Rodriguez, Ana). (Entered: 08/02/2012)
07/27/2012		Notice of Hearings: Because of a conflict in the Court's calendar, the Status Conference set for 7/31/2012 is rescheduled to 11:00 AM in Courtroom 6B South before Judge Sterling Johnson Jr. (Rodriguez, Ana) (Entered: 07/27/2012)
06/29/2012	31	AMENDED COMPLAINT against John Does 1-39, filed by National Automated Clearinghouse Association, Microsoft Corp., FS-ISAC, Inc.. (Attachments: # 1 Appendix A, # 2 Appendix B, # 3 Appendix C, # 4 Appendix D, # 5 Appendix E) (Jacobsen, Richard) (Entered: 06/29/2012)
06/29/2012	30	NOTICE of Voluntary Dismissal by FS-ISAC, Inc., Microsoft Corp., National Automated Clearinghouse Association . *Notice of Dismissal of John Doe 36* (Jacobsen, Richard) (Entered: 06/29/2012)
06/29/2012	29	STATUS REPORT by FS-ISAC, Inc., Microsoft Corp., National Automated Clearinghouse Association (Jacobsen, Richard) (Entered: 06/29/2012)
06/29/2012		Set/Reset Hearings: Status Conference set for 6/29/2012 is adjourned to 7/31/2012 09:30 AM in Courtroom 6B South before Judge Sterling Johnson Jr. (Rodriguez, Ana) (Entered: 06/29/2012)
05/04/2012	28	NOTICE OF FILING OF OFFICIAL TRANSCRIPT of Proceedings held on March 29, 2012, before Judge Johnson. Court Reporter/Transcriber H. Driscoll, Telephone number (718)613-2274. Email address: hdrisc@aol.com. Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date it may be obtained through PACER. Redaction Request due 5/25/2012. Redacted Transcript Deadline set for 6/4/2012. Release of Transcript Restriction set for 8/2/2012. (Driscoll, Holly) (Entered: 05/04/2012)
04/23/2012	27	ORDER granting 26 Motion for expedited discovery. (Ordered by Senior Judge Sterling Johnson, Jr on 4/23/2012) (Guzzi, Roseann) (Entered: 04/23/2012)
04/20/2012	26	Notice of MOTION to Amend/Correct/Supplement 24 Order on Motion to Expedite *Discovery* by FS-ISAC, Inc., Microsoft Corp., National Automated Clearinghouse Association. (Attachments: # 1 Motion to Amend Order for Expedited Discovery, # 2 Declaration of Richard A. Jacobsen in Support of Motion to Amend Order for Expedited Discovery, # 3 [Proposed] Amended Order Granting Motion for Expedited Discovery) (Jacobsen, Richard) (Entered: 04/20/2012)
04/04/2012		Email Notification Test - DO NOT REPLY (Lee, Tiffeny) (Entered:

		04/04/2012)
04/04/2012		Email Notification Test - DO NOT REPLY (Lee, Tiffeny) (Entered: 04/04/2012)
04/04/2012	25	NOTICE of Appearance by Gabriel M. Ramsey on behalf of All Plaintiffs (notification declined or already on case) (Ramsey, Gabriel) (Entered: 04/04/2012)
04/04/2012	24	ENDORSED ORDER granting with modification 23 Motion to Expedite Discovery. A status report must be filed by June 29, 2012. Ordered by Magistrate Judge Roanne L. Mann on 4/4/2012. (Maynard, Pat) (Entered: 04/04/2012)
04/03/2012	23	Notice of MOTION to Expedite *Discovery to Identify Doe Defendants* by FS-ISAC, Inc., Microsoft Corp., National Automated Clearinghouse Association. (Attachments: # 1 Motion For Expedited Discovery To Identify Doe Defendants, # 2 Proposed Order) (Jacobsen, Richard) (Entered: 04/03/2012)
03/29/2012		Minute Entry for proceedings held before Senior Judge Sterling Johnson, Jr: Case called. Counsel Gabriel Ramsy appearing for plaintiff. Show Cause Hearing held on 3/29/2012. Plaintiff's application for a Preliminary Injunction is granted. Plaintiff's request for additional 90 days for discovery regarding ID of defendants is granted. Status Conference set for 6/29/2012 09:30 AM in Courtroom 6B South before Senior Judge Sterling Johnson Jr. (Court Reporter Holly Driscoll.) (Rodriguez, Ana) (Entered: 04/05/2012)
03/29/2012	22	ORDER FOR PRELIMINARY INJUNCTION. (Ordered by Senior Judge Sterling Johnson, Jr on 3/29/2012) (Guzzi, Roseann) (Entered: 03/29/2012)
03/28/2012	18	NOTICE by FS-ISAC, Inc., Microsoft Corp., National Automated Clearinghouse Association re 13 Order to Show Cause, Temporary Restraining Order, Preliminary Injunction */[Proposed] Order for Preliminary Injunction* (Attachments: # 1 Appendix A-1, # 2 Appendix A-2, # 3 Appendix B, # 4 Appendix C) (Jacobsen, Richard) (Entered: 03/28/2012)
03/28/2012		Notice of Hearings:The Show Cause Hearing set for 3/29/2012 will be heard at 09:30 AM in Courtroom 6B South before Senior Judge Sterling Johnson Jr. (Rodriguez, Ana) (Entered: 03/28/2012)
03/28/2012		ORDER REASSIGNING CASE. Case reassigned by random selection to Senior Judge Sterling Johnson, Jr for all further proceedings. Chief Judge Carol Bagley Amon no longer assigned to case. Ordered by Chief Judge Carol Bagley Amon on 3/28/2012. (Palmer, Douglas) (Entered: 03/28/2012)
03/27/2012	17	SCHEDULING ORDER: re 13 Order to Show Cause, Temporary Restraining Order, Preliminary Injunction, (Show Cause Hearing set for 3/29/2012 10:00 AM in Courtroom 10D South before Chief Judge Carol Bagley Amon.)LOCATION CHANGE: The hearing on Plaintiff's motion for a preliminary injunction previously set for March 29, 2012 at 10 AM in Courtroom 636 will be held at the same date and time in Courtroom 10D South before Judge Carol B. Amon. Ordered by Chief Judge Carol Bagley Amon on 3/27/2012. (Shnider, Ruth) (Entered: 03/27/2012)

03/27/2012	16	(Show Cause Hearing set for 3/29/2012 10:00 AM in Courtroom 10D South before Chief Judge Carol Bagley Amon.), SCHEDULING ORDER: re 13 Order to Show Cause, Temporary Restraining Order, Preliminary Injunction LOCATION CHANGE: The hearing on Plaintiff's motion for a preliminary injunction previously set for March 29, 2012 at 10 AM in Courtroom 636 will be held at the same date and time in Courtroom 10D South before Judge Carol B. Amon. Ordered by Chief Judge Carol Bagley Amon on 3/27/2012. (Shnider, Ruth) (Entered: 03/27/2012)
03/27/2012	15	Order to Unseal CasePursuant to the Order to Temporarily Seal Case entered by Judge William F. Kuntz on March 19, 2012, and the Notice of Execution of Ex Parte Temporary Restraining Order and Seizure Order filed by the plaintiffs on March 27, 2012, it is hereby ordered that the above-captioned case be immediately unsealed, such that all case materials previously filed under seal be accessible on the public docket. Ordered by Chief Judge Carol Bagley Amon on 3/27/2012. (Shnider, Ruth) (Entered: 03/27/2012)
03/27/2012	14	NOTICE OF EXECUTION OF EX PARTE TEMPORARY RESTRAINING ORDER AND SEIZURE ORDER (Fernandez, Erica) (Entered: 03/27/2012)
03/22/2012		ORDER ORDER OF RECUSAL. Judge William F. Kuntz, II recused. Case reassigned to Chief Judge Carol Bagley Amon for all further proceedings. Ordered by Judge William F. Kuntz, II on 3/22/2012. (Gapinski, Michele) (Entered: 03/22/2012)
03/21/2012		ORDER REASSIGNING CASE. Case reassigned to Judge William F. Kuntz, II for all further proceedings. Senior Judge Edward R. Korman no longer assigned to case. Ordered by Chief Judge Carol Bagley Amon on 3/21/2012. (Bowens, Priscilla) (Entered: 03/21/2012)
03/19/2012	21	DECLARATION OF WILLIAM D. JOHNSON in support of 12 Plaintiffs' Application for an Emergency Temporary Restraining Order, Seizure Order and Order to Show Cause for Preliminary Injunction by FS-ISAC, Inc., Microsoft Corp., National Automated Clearinghouse Association. (Fernandez, Erica) (Entered: 03/29/2012)
03/19/2012	20	DECLARATION OF Jesse D. Kornblum in Support of 12 Plaintiffs' Application for an Emergency Temporary Restraining Order, Seizure Order and Order to Show Cause for Preliminary Injunction by FS-ISAC, Inc., Microsoft Corp., National Automated Clearinghouse Association (Fernandez, Erica) (Main Document 20 replaced on 3/29/2012) (Fernandez, Erica). (Entered: 03/29/2012)
03/19/2012	19	BRIEF in Support of 12 Plaintiffs' Application for an Emergency Temporary Restraining Order, Seizure Order and Order to Show Cause for Preliminary Injunction filed by FS-ISAC, Inc., Microsoft Corp., National Automated Clearinghouse Association. (Fernandez, Erica) (Entered: 03/29/2012)
03/19/2012	13	EX-PARTE TEMPORARY RESTRAINING ORDER, SEIZURE ORDER AND ORDER TO SHOW CAUSE re PRELIMINARY INJUNCTION (Appendix A-C attached in hard copy). Ordered by Judge William F. Kuntz, II on 3/19/2012. (Fernandez, Erica) (Entered: 03/27/2012)
03/19/2012	12	PLAINTIFFS' EX PARTE APPLICATION for an Emergency Temporary

		Restraining Order, Seizure Order, and Order to Show Cause re Preliminary Injunction. Ordered by Judge William F. Kuntz, II on 3/19/2012. (Fernandez, Erica) (Entered: 03/27/2012)
03/19/2012	11	ORDER granting 6 Motion to TEMPORARILY Seal Case. Ordered by Judge William F. Kuntz, II on 3/19/2012. (Fernandez, Erica) (Entered: 03/27/2012)
03/19/2012	10	PLAINTIFFS' APPLICATION BY ORDER TO SHOW CAUSE endorsed on doc 2 filed by FS-ISAC, Inc., National Automated Clearinghouse Association, Microsoft Corp. Ordered by Judge William F. Kuntz, II on 3/19/2012. (Fernandez, Erica) (Entered: 03/27/2012)
03/19/2012	9	ORDER granting 5 Motion for Leave to Appear Pro Hac Vice. Ordered by Magistrate Judge Roanne L. Mann on 3/19/2012. (Greene, Donna) (Entered: 03/19/2012)
03/19/2012	8	ORDER granting 4 Motion for Leave to Appear Pro Hac Vice. Ordered by Magistrate Judge Roanne L. Mann on 3/19/2012. (Greene, Donna) (Entered: 03/19/2012)
03/19/2012	7	ORDER granting 3 Motion for Leave to Appear Pro Hac Vice. Ordered by Magistrate Judge Roanne L. Mann on 3/19/2012. (Greene, Donna) (Entered: 03/19/2012)
03/19/2012		FILING FEE: $ 350, receipt number 4653041353 (Bowens, Priscilla) (Entered: 03/19/2012)
03/19/2012	6	MOTION to Seal Case by FS-ISAC, Inc., Microsoft Corp., National Automated Clearinghouse Association. (Bowens, Priscilla) (Entered: 03/19/2012)
03/19/2012		FILING FEE: $ 25, receipt number 4653041355 (Bowens, Priscilla) (Entered: 03/19/2012)
03/19/2012	5	MOTION for Leave to Appear Pro Hac Vice by FS-ISAC, Inc., Microsoft Corp., National Automated Clearinghouse Association. (Bowens, Priscilla) (Entered: 03/19/2012)
03/19/2012		FILING FEE: $ 25, receipt number 4653041357 (Bowens, Priscilla) (Entered: 03/19/2012)
03/19/2012	4	MOTION for Leave to Appear Pro Hac Vice by FS-ISAC, Inc., Microsoft Corp., National Automated Clearinghouse Association. (Bowens, Priscilla) (Entered: 03/19/2012)
03/19/2012		FILING FEE: $ 25, receipt number 4653041356 (Bowens, Priscilla) (Entered: 03/19/2012)
03/19/2012	3	MOTION for Leave to Appear Pro Hac Vice by FS-ISAC, Inc., Microsoft Corp., National Automated Clearinghouse Association. (Bowens, Priscilla) (Entered: 03/19/2012)
03/19/2012	2	Unsigned Order to Show Cause by FS-ISAC, Inc., Microsoft Corp., National Automated Clearinghouse Association (Bowens, Priscilla) (Entered: 03/19/2012)
03/19/2012	1	COMPLAINT against All Defendants Disclosure Statement on Civil Cover Sheet completed -yes,, filed by National Automated Clearinghouse

		Association, Microsoft Corp., FS-ISAC, Inc.. (Attachments: # 1 Civil Cover Sheet, # 2 Appendix A, # 3 Appendix B, # 4 Appendix C, # 5 Appendix D, # 6 Appendix E, # 7 Summons John Doe 1, # 8 Summons John Doe 2, # 9 Summons John Doe 3, # 10 Summons John Doe 4, # 11 Summons John Doe 5, # 12 Summons John Doe 6, # 13 Summons John Doe 7, # 14 Summons John Doe 8, # 15 Summons John Doe 9, # 16 Summons John Doe 10, # 17 Summons John Doe 11, # 18 Summons John Doe 12, # 19 Summons John Doe 13, # 20 Summons John Doe 14, # 21 Summons John Doe 15, # 22 Summons John Doe 16, # 23 Summons John Doe 17, # 24 Summons John Doe 18, # 25 Summons John Doe 19, # 26 Summons John Doe 20, # 27 Summons John Doe 21, # 28 Summons John Doe 22, # 29 Summons John Doe 23, # 30 Summons John Doe 24, # 31 Summons John Doe 25, # 32 Summons John Doe 26, # 33 Summons John Doe 27, # 34 Summons John Doe 28, # 35 Summons John Doe 29, # 36 Summons John Doe 30, # 37 Summons John Doe 31, # 38 Summons John Doe 32, # 39 Summons John Doe 33, # 40 Summons John Doe 34, # 41 Summons John Doe 35, # 42 Summons John Doe 36, # 43 Summons John Doe 37, # 44 Summons John Doe 38, # 45 Summons John Doe 39, # 46 Proposed Order Temporary, # 47 EX PARTE Application for Emergency TRO, # 48 Declaration Debenham, # 49 Exhibit Debenham, # 50 Declaration Heath, # 51 Exhibit Heath1-5, # 52 Exhibit Heath 6, # 53 Exhibit Heath 7, # 54 Exhibit Heath 8,9, # 55 Exhibit Heath 10, # 56 Exhibit Heath 11-19, # 57 Declaration Johnson, # 58 Exhibit Johnson, # 59 Declaration Kornblum, # 60 Exhibit Kornblum, # 61 Declaration Moore, # 62 Exhibit Moore, # 63 Declaration Nelson, # 64 Exhibit Nelson, # 65 Memo, # 66 Proposed Ex Parte TRO, # 67 Proposed Order Appendix A, # 68 Proposed Order Appendix B, # 69 Proposed Order Appendix C) (Bowens, Priscilla) (Entered: 03/19/2012)

PACER Service Center

Transaction Receipt

11/26/2012 15:01:01

PACER Login:	oh0152	**Client Code:**	
Description:	Docket Report	**Search Criteria:**	1:12-cv-01335-SJ-RLM
Billable Pages:	8	**Cost:**	0.80