IN THE UNITED STATES DISTRICT COURT

FOR THE WESTERN DISTRICT OF NORTH CAROLINA

CHARLOTTE DIVISION

MICROSOFT CORPORATION, Plaintiff, v. JOHN DOES 1-82, CONTROLLING A COMPUTER BOTNET THEREBY INJURING MICROSOFT AND ITS CUSTOMERS, Defendant.	Civil Action No. 3:13-CV-00319-GCM **MOTION FOR DEFAULT JUDGMENT AND PERMANENT INJUNCTION**

Plaintiff Microsoft Corp. ("Microsoft") respectfully moves the Court to grant default judgment and issue a permanent injunction against Defendant John Does 1-82, who operated and controlled the Citadel botnets from and through the Internet domain names identified in Appendix A to the Proposed Order, filed herewith.

The Citadel botnets have infected a very large number of Internet users' computers. (Complaint, Dkt. No. 2, ¶¶ 10-15, 18-48) Various fraudulent techniques are used to lure victims to websites from which malicious botnet code is surreptitiously installed on their computers. (*Id.*, ¶ 39) 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. (*Id.*, ¶¶ 52-74) The botnet code then waits for the unsuspecting user to utilize online banking websites and, when they do so, takes control of the Internet browser and intercepts the user's credentials. (*Id.* ¶¶ 63-69) The user's credentials are then used to steal money from their bank accounts. (*Id.*)

Default judgment is warranted here. Microsoft served Defendants with its Complaint and summons and related materials through e-mail, electronic messaging and publication, which are Court-ordered methods pursuant to Fed. R. Civ. P. 4(f)(3). On October 25, 2013, the Clerk of Court entered default against Defendants. (Dkt. No. 20)

Pursuant to Fed. R. Civ. P. 55(b)(2), Microsoft seeks default judgment and a permanent injunction against Defendants: (1) prohibiting Defendants from operating or propagating the Citadel botnets, and (2) transferring ownership and control of the botnet command and control domains to Microsoft. This relief is necessary to prevent the botnet control infrastructure from coming back online, to prevent new computers from being infected and to enable Microsoft to work toward disinfecting end-user computers.

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 Microsoft seeks only non-monetary relief at this point. Issues of substantial public importance weigh heavily in favor of a permanent injunction as, without the requested relief, the botnet would be able to resume its injurious operations. There are no disputed material issues of fact; Microsoft adduced overwhelming evidence of the alleged activities, which was set forth in detail in the Complaint (Dkt. No. 2), and Defendants have not 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 over five months, despite repeated service and communications directed to them. Microsoft will be prejudiced unless default judgment and a permanent injunction are issued, given that in the absence of such relief the botnets will be able to continue to injure Microsoft, its customers, as well as the public at large. Finally, default judgment and a permanent injunction will not impact any legitimate interests, as the domains affected are those used in the botnet's illegal operations. Moreover, to the extent that the assistance of third party domain registries and registrars is needed to effect final relief against Defendants, the Court has authority under the All Writs Act to direct such limited relief.

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

I. STATEMENT OF FACTS

A. Procedural History

Microsoft filed this suit on May 29, 2013, alleging that Defendants controlled a large number of Internet domains, as the "command and control" infrastructure for the Citadel botnets. Microsoft alleged that the deleterious effects of the botnets caused and continued to cause irreparable injury to Microsoft, its customers and members of the public, and stated claims for violation of the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the CAN-SPAM Act (15 U.S.C. § 7704); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 et seq.); the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); North Carolina General Statute § 14-458 (Computer Trespass); and the common law of conversion, unjust enrichment, and nuisance.

Simultaneously, Microsoft applied for an Emergency Temporary Restraining Order and preliminary injunction to disable the Citadel botnets command and control server software, operating from and through the domains at issue in this case. The Court issued a Temporary Restraining Order, Seizure Order and Order to Show Cause Re Preliminary Injunction (the "TRO") on May 29, 2013. The order was executed on June 5, 2013 – all of the domains were disabled, and Defendants' software operating at and through these domains was, thus, disabled. On June 11, 2013, the Court issued a Preliminary Injunction transferring to Microsoft's control, during the pendency of this action, the domains through which the Defendants operated and controlled the Citadel botnets.

When it issued the TRO and Preliminary Injunction, the Court found good cause to permit service of Microsoft's Complaint and related materials by alternative means pursuant to Rule 4(f)(3). The Court has directed that, under the circumstances, appropriate means of service

authorized by law, satisfying Due Process, and reasonably calculated to notify Defendants of this action, included transmission by electronic messaging and e-mail and other contact information associated with Defendants or provided by Defendants to domain registrars and Internet hosting providers who provided services that were used by Defendants to host the Citadel command and control infrastructure and publication of notice of these proceedings on a publicly available Internet website. The Court further granted Microsoft the ability to pursue discovery, in order to obtain further contact and identifying information regarding Defendants.

Despite being served the Complaint, summons and other pleadings in the action over the course of many months, Defendants have not responded to the complaint or appeared in the action. Accordingly, on October 25, 2013, the Clerk of Court entered default against them (Dkt. No. 20).

B. Enjoining Defendants' Illegal Activities And Transferring The Botnet Domains To Microsoft Will Prevent The Harm Caused By The Botnet

The Internet domains 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 Citadel botnets. (*See* Dkt. No. 2, ¶¶ 47-48 and Appx. A) Microsoft set forth detailed evidence establishing this fact in the Complaint and in connection with Microsoft's motion for the TRO. (*See* Dkt. Nos. 2 and 9) All such factual material is incorporated by reference, in support of this motion.

The permanent injunction sought by Microsoft directs that Defendants cease their malicious conduct, and directs that the domains constituting the infrastructure of the Citadel botnets be transferred to Microsoft's ownership and control. This will ensure that the Citadel botnets will not be able to continue their injurious operations. Further, providing the requested relief will allow Microsoft time to identify and clean the installed base of infected computers, both through Microsoft's own relationships with its customers and through Microsoft's partnering with relevant Internet service providers providing connectivity for such computers.

The result will be that the network of infected computers will be dismantled and, at a future date, the domains will 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. *Park Corp. v. Lexington Ins. Co.,* 812 F.2d 894, 896 (4th Cir. 1987); *United States CFTC v. PMC Strategy*, LLC, 903 F. Supp. 2d 368, 375 (W.D.N.C. 2012) ("Entry of default judgment is left to the sound discretion of the trial court."); *Duke Energy Carolinas, LLC v. BlackRock Coal, LLC*, 2012 U.S. Dist. LEXIS 43413 (W.D.N.C. 2012) (granting default judgment in plaintiff's favor after finding that service of the complaint and summons on defendant was sufficient yet defendant failed to defend). 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; the effect of a default judgment; or whether the default was caused by a good-faith mistake or by excusable or inexcusable neglect on the part of the defendant." *Id.*; *see also* Wright, Miller & Kane, Federal Practice and Procedure: Civil 3d § 2685); *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).

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. Microsoft seeks only injunctive relief prohibiting Defendants from operating the Citadel botnets or engaging in any of the malicious conduct alleged in this case. Microsoft also seeks injunctive relief directing the relevant domain registries and registrars to transfer to Microsoft ownership and control of the domains used to control and propagate the Citadel botnets, so that the botnets cannot be revived through those domains.

Second, this case presents a matter of serious public importance. Through operation of the Citadel botnets, Defendants have taken control of a large number of victim computers, have taken control of those users' Microsoft Windows operating system and Internet Explorer browsers, have compromised the functionality of that software and mislead victims into providing personal information and financial credentials, which are used by Defendants to steal the victims' money. (Dkt. No. 2, ¶¶ 16-74) By these actions, Defendants have harmed Microsoft, its customers and the general public. Extending the protective measures put in place as part of the preliminary injunction by permanently transferring ownership and control of the botnet domains to Microsoft will help ensure that the Citadel botnets do not reconnect with the computers infected prior to this lawsuit, will prevent the continued intrusion and misuse of those computers and will permit Microsoft time to facilitate the cleaning of those computers.

The possibility of a disputed issue regarding material facts is a remote one. Microsoft, in its detailed Complaint, pleadings and accompanying declarations have adduced incontrovertible and overwhelming evidence that the domains at issue were used to control and propagate the Citadel botnets. (*See* Dkt. Nos. 2, 9) Despite being served, Defendants have not appeared or otherwise attempted 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 operation of the Citadel

botnets violated the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the CAN-SPAM Act (15 U.S.C. § 7704); violated the Electronic Communications Privacy Act (18 U.S.C. § 2701); constituted Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 et seq.); violated the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); violated North Carolina General Statute § 14-458 (Computer Trespass); and violated the common law of conversion, unjust enrichment, and nuisance. (*See* Dkt. No. 2, ¶¶ 75-167)

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. Microsoft has made extraordinary efforts over the course of many months to ensure that Defendants been provided notice and the opportunity to appear, and the evidence indicates that Defendants are aware of this action, but have chosen not to respond. (*See* Dkt. Nos. 17-19)

Fourth, Microsoft, along with the other victims of the Citadel botnets, has been prejudiced by Defendants delay in this lawsuit, insofar as the Defendants have refused to respond to Microsoft's complaint in any manner whatsoever; have refused to engage in discovery or provide any manner of justification for their conduct; have delayed the ability of Microsoft to take final control of the Citadel botnet infrastructure and have refused to assist Microsoft in identifying, much less in recompensing, the wholly innocent victims of their acts.

Fifth, the grounds for default are clearly established. Even five months after Microsoft filed its complaint, disabled the botnet technical infrastructure—thousands of domains—by order of the Court, and launched extensive efforts to identify and serve Defendants, they have made no appearance in this case and have made no response whatsoever to the complaint. Microsoft went to extraordinary lengths to provide notice of this lawsuit to Defendants—sending notice to *thousands* of Defendants' email and messaging addresses. Certain of the Defendants—in particular John Doe 1, who is responsible for the entire Citadel scheme—did ultimately respond

to Microsoft's 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. Microsoft seeks only transfer of ownership and control of the botnet domains, effectively continuing the measures already protecting the public through the Court's preliminary injunction. The current control exerted over the Citadel botnet domains disable the operation of the Citadel botnets while causing the least amount of burden on third party domain registries and registrars responsible for administering those domains.

Seventh, Defendants' default is not the result of excusable neglect. Microsoft went to extraordinary lengths to provide notice of this lawsuit to them. (*See* Dkt. Nos. 17-19) It is quite evident 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 Microsoft's 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 factual substance 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 domain name and hosting facilities in this country, and in other countries, should not be able to evade judgment and continue to harm Microsoft and the U.S. public merely because they have been successful in operating the Citadel botnets from overseas.

1. Microsoft Has Sufficiently Pled Its Claims

Microsoft's Complaint sets forth in detail the legal and factual bases for the following statutory and common law claim: (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) computer trespass, (9) conversion, (10) unjust enrichment; and (11) nuisance.

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 Microsoft and its Windows operating system running on computers 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 Citadel Botnets intentionally access without authorization Microsoft's email servers (to send huge volumes of unsolicited, malicious spam email to Microsoft's customers). The Citadel Botnets intentionally access without authorization the servers of third-parties, including financial institution members, in order to access financial accounts and steal funds from these institutions and victim computer users. (Dkt. No. 2, ¶¶ 21-74, 75-80)

[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).

The Citadel Botnets' intentional unauthorized access of Microsoft's protected computers, moreover, has resulted in substantial damages and loss, including the costs associated with investigating the unauthorized access. The Complaint demonstrates that Microsoft and its customers are damaged by this unauthorized intrusion. Performance and operation of victim computers and Microsoft's software is degraded by the Citadel Botnets' intrusion. Microsoft's email servers are burdened by the sending of an enormous amount of spam email. Microsoft and other members of the public must invest considerable time and resources investigating and remediating the Defendants' intrusion into these computers. Microsoft must spend time and resources to combat and remediate infections of user computers caused by the Citadel Botnets. (Dkt. No. 2, ¶¶ 49-74, 75-80)

The Citadel Botnets' unauthorized access is precisely the type of activity the Computer Fraud and Abuse Act is designed to prevent. *See e.g. WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012) (CFAA is "designed to combat hacking"); *Big Rock Sports LLC v. Acusport Corp.*, 2011 U.S. Dist. LEXIS 110995, *4 (E.D.N.C. 2011) ("The CFAA penalizes 'access' or intrusions to a computer system…"); *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); *Physicians Interactive v. Lathian Sys., Inc.,* 2003 U.S. Dist. LEXIS 22868, *25 (E.D. Va. 2003) (granting TRO and preliminary injunction under CFAA where the defendant hacked into a computer and stole confidential information); *America Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 451 (E.D. Va. 1998) (defendant's unauthorized access of plaintiff's servers violated CFAA); *Facebook, Inc. v. Fisher*, 2009 U.S. Dist. LEXIS 122578 (N.D. Cal. 2009) (granting a TRO under CFAA where defendants allegedly engaged in a phishing (stealing sensitive information by masquerading as a reliable source) and spamming scheme that compromised the accounts of

Facebook users).[2] Accordingly, Microsoft has stated a claim and is likely to succeed on the merits of its Computer Fraud and Abuse Act claim.

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, or third party financial institutions, NACHA and other companies, or other false addresses, thereby disguising their origin with the purpose of misleading recipients and evading detection. (Dkt. No. 2, ¶¶ 49-74, 81-92). This is precisely what CAN-SPAM prohibits. *See Aitken v. Communs. Workers of Am.*, 496 F. Supp. 2d 653, 667 (E.D. Va. 2007) (inaccurate "from" line and header information may violate CAN-SPAM); *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). Microsoft therefore states a claim and is likely to succeed on the merits of its 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

[2] Indeed, in recent years botnet operators who disseminate code that intrudes upon user computers, collects personal information and causes injury have been indicted and convicted criminally under the Computer Fraud & Abuse Act. *See* Dkt. 9, Cox Decl. ¶¶ 36-37, Exs. 10 (Indictment of Jeanson James Ancheta), 37 (Sentencing of Jeanson James Ancheta).

authorized access to an electronic communication while it is in electronic storage. 18 U.S.C. § 2701(a). Microsoft's licensed Windows operating system on end-user computers and servers of third-party financial institutions are facilities through which electronic communication services are provided. The Citadel Botnets' malicious code, installed without authorization on infected computers, searches emails and other files, intercepts user communications to and from websites, 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. 2, ¶¶ 49-74, 93-98) Obtaining stored electronic information in this way, without authorization, is a violation of the Electronic Communications Privacy Act. *See Global Policy Partners, LLC*, 2009 U.S. Dist. LEXIS 112472 at *9-13 (unauthorized access to emails was actionable under ECPA); *State Analysis, Inc. v. American Fin. Srvcs. Assoc.*, 621 F. Supp. 2d 309, 317-18 (E.D. Va. 2009) (access of data on a computer without authorization actionable under ECPA); *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC,* 759 F. Supp. 2d 417 (S.D.N.Y. 2010) (unauthorized access of emails stored on a third-party communication service provider system violated the ECPA), *cited with approval Bryan v. Bryan*, 2012 U.S. Dist. LEXIS 150648, *1-2 (W.D.N.C. 2012). Microsoft therefore states a claim and is likely to succeed on the merits of its Electronic Communications 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 Microsoft's registered, famous and distinctive trademarks in fraudulent versions of its Windows operating system and Internet Explorer browser, which deceive victims, causing them confusion and causing them to mistakenly associate Microsoft with this

activity. Defendants similarly misuse the trademarks of third party financial institutions, NACHA and other institutions as well. (Dkt. No. 2, ¶¶ 16-74, 99-118)

The Citadel Botnet also makes such use of trademarks in website templates and spam templates that Defendants then use to mislead Internet users into providing their 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. (*Id.*) This is a clear violation of the Lanham Act and Microsoft is likely to succeed on the merits. *See American Angus Ass'n v. Sysco Corp.*, 829 F. Supp. 807, 820 (W.D.N.C. 1992) (granting preliminary injunction where defendant's use of mark was likely to cause confusion); *IHOP Corp. v. Langley*, 2008 U.S. Dist. LEXIS 112056, *1-3 (E.D.N.C. 2008) (granting TRO where defendant's use of mark was likely to cause confusion); *Audi AG v. Shokan Coachworks, Inc.,* 592 F. Supp. 2d 246, 279 (N.D.N.Y. 2008) (holding that the use of the plaintiffs' marks in the defendants' email addresses created a likelihood of consumer confusion); *Brookfield Commc'ns. v. W. Coast Entm't Corp.*, 174 F.3d 1036, 1066-1067 (9th Cir. 1999) (entering preliminary injunction under 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 Citadel Botnets' misleading and false uses of Microsoft's trademarks—including "Microsoft," "Windows," "Internet Explorer"—and also the trademarks of third parties including "NACHA," the NACHA logo, "Bank of America," "Wells Fargo," "Citibank," and others, causing confusion and mistake as to affiliation with the malicious conduct carried out by the botnet. (Dkt. No. 2, ¶¶ 16-74, 99-118) This activity is a clear violation of Lanham Act § 1125(a) and Microsoft is likely to succeed on the merits. *See*

Garden & Gun, LLC v. Twodalgals, LLC, 2008 U.S. Dist. LEXIS 79982 (W.D.N.C. 2008) (granting preliminary injunction against misleading use of trademarks under Section 1125(a)); *IHOP Corp.*, 2008 U.S. Dist. LEXIS 112056 at *1-3 (same; granting TRO); *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); also constituted trademark "dilution" under §1125(c)); *Brookfield Commc'ns.,* 174 F. 3d at 1066-67 (entering preliminary injunction under Lanham Act §1125(a) for infringement of trademark in software and website code); *Hotmail Corp. v. Van$ Money Pie, Inc.*, 1998 U.S. Dist. LEXIS 10729, *12-13 (N.D. Cal. 1998) (granting preliminary injunction; copying the Hotmail trademarks in "e-mail return addresses" constituted false designation of origin; also constituted trademark "dilution" under §1125(c)).

Microsoft therefore states claims under the Lanham Act and is likely to succeed on the merits of its claims.

e. Defendants' Computer Trespass /Conversion

A trespass to chattels occurs where a defendant interferes, unlawfully and without authorization, or dispossesses the personal property in the plaintiff's possession. *Fordham v. Eason*, 351 N.C. 151, 155 (1999). In particular, prohibitions on "Computer Trespass" have been enacted by statute at North Carolina General Statutes § 14-458. This provision prohibits, among other things, a defendant, without authority, from using a computer to "alter… computer programs, or computer software" or "to cause physical injury to the property of another" and defines such as a trespass. N.C. Gen. Stat. § 14-458(a)(3), (4). Similarly, conversion occurs where a defendant makes an unauthorized assumption and exercise of the right of ownership over goods belonging to another, to the alteration of their condition or the exclusion of the owner's rights. *Peed v. Burleson's, Inc.*, 244 N.C. 437, 439 (1956).

Defendants have intruded upon, interfered with and taken as their own Microsoft's resources and property, by (1) altering, interfering with, installing software within and causing injury to Microsoft's licensed Windows operating system on victim computers and (2) interfering with and intruding upon Microsoft's Hotmail servers to which Defendants send vast

quantities of spam e-mail. (Dkt. No. 2, ¶¶ 49-74, 135-150) These activities injure the value of Microsoft's property and constitute a trespass and conversion. *See* N.C. Gen. Stat. § 14-458(a)(3), (4); *Bridgetree, Inc. v. Red F Mktg. LLC*, 2013 U.S. Dist. LEXIS 15372, *45-51 (W.D.N.C. 2013) (defendants liable under North Carolina law for conversion of computer files where they were not authorized to own the files and excluded the owner from exercising right of ownership and control over them); *Springs v. Mayer Brown, LLP*, 2012 U.S. Dist. LEXIS 9734 (W.D.N.C. 2012) (under North Carolina law, conversion could be predicated on taking a copy of a computer file, as it deprived plaintiff from control over its property); *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) (TRO and preliminary injunction where defendant hacked computers and obtained proprietary information). Microsoft therefore states claims for computer trespass and conversion, and is likely to succeed on the merits of those claims.

f. Defendants' Unjust Enrichment

The elements of a claim of unjust enrichment are that a (1) defendant benefitted, (2) the benefit was not gratuitous, (3) the benefit is measurable, and (4) the defendant consciously accepted the benefit. *Carty v. Westport Homes of N.C., Inc.*, 472 Fed. Appx. 255, 258-9 (4th Cir. 2012) (citing *Booe v. Shadrick*, 322 N.C. 567, 570 (1988)). Defendants controlling the Citadel Botnets have benefited from Microsoft's Windows operating system, Internet Explorer browser, and servers as well as its trademarks, brand names, and goodwill by, among other things, intruding upon and converting for their own use Microsoft's property, to further Defendants' banking fraud on users of Microsoft's Windows operating system. (Dkt. No. 2, ¶¶ 49-74, 151-161) Defendants have specifically taken, without authorization, the benefit of Microsoft's software in order to steal information and money. In each instance, Defendants have profited from their unlawful activity, reaping millions of dollars in stolen money and information. Thus, it is certainly inequitable for Defendants controlling the Citadel Botnets to

retain these benefits. Accordingly, Microsoft states a claim for unjust enrichment and is likely to succeed on the merits.

g. Defendants' Liability For Nuisance

"[A] private nuisance exists in a legal sense when one makes an improper use of his own property and in that way injures the land or some incorporeal right of one's neighbor." *Morgan v. High Penn Oil Co.*, 238 N.C. 185, 193 (1953) (citations omitted); *Evans v. Lochmere Rec. Club*, 176 N.C. App. 724, 727-728 (N.C. Ct. App. 2006) (stating claim for nuisance where defendant "has used amplified sound from speakers aimed directly at [plaintiffs'] premises"). A private nuisance action may arise from the defendant's intentional and unreasonable conduct or it may be grounded in negligence. *Pendergrast v. Aiken*, 293 N.C. 201, 236 S.E. 2d 787 (1977); Restatement (Second) of Torts Sec. 822 (1979).

Here, Defendants operating software on victim computers have intentionally directed their malicious activities and misused their property and the property of others, in a manner that injures the rights of Microsoft. (Dkt. No. 2, ¶¶ 49-74, 162-167) Defendants' conduct is highly unreasonable, has no social value and thus constitutes a nuisance, which should be abated by the injunctive relief sought herein. *See Mayes v. Tabor*, 77 N.C. App. 197, 199-201 (N.C. Ct. App. 1985) (error to deny injunction to abate a nuisance).

h. 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).

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. 2, ¶¶ 16-74, 119-134) Microsoft states claims for Defendants' RICO violations and is likely to succeed on the merits of those claims.

(1) The Citadel Enterprise

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 Citadel Enterprise has existed since at least January 2012, when John Doe 1 began offering the Citadel botnet kit to John Does 2-82. (Dkt. No. 2, ¶¶ 22-44) John Does 2-82 joined and began participating in the Citadel Enterprise at various times thereafter. (*Id.*). *See United States v. Banks*, 10 F.3d 1044, 1053-54 (4th Cir. 1993) (single conspiracy found even where loose organizational structure, changing membership, shifting roles of participants, limited roles and knowledge of some members). The Citadel 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 Microsoft requests. (Dkt. No. 2, ¶¶ 22-44)

Defendants' interrelated roles in the operation of the Citadel Botnets, in furtherance of common financial interests, demonstrate the purpose of the Citadel 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"). The relationship between Defendants may also be inferred by the Defendants' development and/or purchasing of the Citadel botnet code and their use of the Citadel botnet system to steal and exploit credentials and money. (Dkt. No. 2, ¶¶ 22-44)

(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). The threat of continuity of interrelated acts may be inferred from "past conduct that by its nature projects into the future with a threat of repetition." *H.J. Inc.* at 241; *Eplus Tech., Inc. v. Aboud*, 313 F.3d 166, 181-182 (4th Cir. Va. 2002). Defendants have conspired to, and have, conducted and participated in the operations of the Citadel 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 Citadel Enterprise. These acts are continuing and will continue unless enjoined.

Defendants' acts of racketeering activity include access device fraud, in violation of 18 U.S.C. § 1029. Whoever "knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices" or "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)(1) & (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 used an unauthorized access device in the form of an unauthorized Windows XP product key to install a stolen copy of Windows XP in order to produce the necessary Citadel botnet software operated by Defendants. (Dkt. No. 2, ¶¶ 49-50) A product key is an authorization code used to "unlock" and gain access to Microsoft Windows, or other software, and thus grants users access to the valuable services provided by the software. Such an authorization code can be considered an "access device" under 18 U.S.C. § 1029(e)(1). *See United States v. Brewer*, 835 F.2d 550, 553 (5th Cir. 1987) (finding access codes used to access a phone system to make long distance calls to be an "access device" under 18 U.S.C. § 1029(e)(1)); *accord United States v. Barrington*, 648 F.3d 1178, 1201 n.23 (11th Cir. 2011) ("[W]e have broadly constructed the definition of access device to include 'innovative means that parties use to gain unauthorized information to engage in fraudulent activities.'"). Further, an authorization code can be considered "counterfeit" or "unauthorized" even if it is accepted by the software as legitimate. *See Brewer*, 835 F.2d at 554 (finding that a code could be counterfeit even if they were legitimately accepted in the same way that a fake credit card is no less counterfeit just because it happens to match a valid account).

Congressional intent indicates that the term "access device" should be broadly construed to accommodate technological changes and advances. *See Brewer*, 835 F.2d at 553 n.1 (citing S. Rep. No. 98-368, 98th Cong., 2d Sess., *reprinted in* 1984 U.S. Code Cong. & Ad. News 3182, 3647, at 3655; H.R. Rep. No. 98-894, 98th Cong., 2d Sess., *reprinted in* 1984 U.S. Code Cong. & Ad. News 3689, at 3705) (noting that the legislative history of § 1029 indicates that Congress wanted the statute to be "broad enough to encompass technological advances."); *see also United States v. Ashe*, 47 F.3d 770, 774 (6th Cir. 1995) (holding that "invasion of an identifiable customer's account is not a necessary element of proof"); *United States v. Bailey*,

41 F.3d 413, 418 (9th Cir. 1994) (holding that nowhere in § 1029 does it "impl[y] that the only 'account' protected against improper access is one maintained by an end consumer.").

As set forth in detail above, Defendants provide a stolen copy of Windows XP as well as an unauthorized product key to provide access to said copy of Windows XP in the Citadel manual to all members of the Citadel Enterprise so that the members can use this copy to build and produce the Citadel botnet software. (Dkt. No. 2, ¶¶ 49-50) Defendants then use the Citadel botnet software, built upon this stolen copy of Windows XP and unauthorized key, to access financial accounts.

Furthermore, Defendants have also 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 Citadel botnet system created and operated by Defendants. (Dkt. No. 2, ¶¶ 31-44) As set forth in detail above, Defendants have used the Citadel botnet system to intrude upon the computers and software of Microsoft and its customers, then 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).[3] Each of these illegal acts was conducted using interstate and/or foreign wires, and therefore affected interstate and/or foreign commerce.[4]

---

[3] 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).

[4] 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. . .

(3) Microsoft's Injury as a Direct Result of Defendants' Pattern of Racketeering Activity

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 Microsoft Hotmail email accounts, with spam messages infringing trademarks, and containing links designed to infect computers with malicious software and steal credentials. As a direct result of Defendants' conduct, Microsoft has been forced to spend resources to mitigate the impact to its customers, and investigate the source of the Citadel botnet and the online identities of Defendants and other members of the Citadel Enterprise. (Dkt. No. 2, ¶¶ 63-74) Accordingly, there is a "direct relation between the injury asserted and the injurious conduct alleged" *Hemi Group, LLC v. City of New York*, 130 S. Ct. 983, 989 (U.S. 2010).[5]

III. CONCLUSION

For all of the foregoing reasons, entry of default judgment and a permanent injunction in favor of Microsoft and against Defendants are appropriate. Microsoft respectfully requests entry of default judgment against Defendants and a permanent injunction prohibiting Defendants from engaging in the conduct underlying this case and directing that the ownership and control of the botnet domains at issue be transferred to Microsoft.

---

communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice.").

[5] 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.*, 553 U.S. 639, 657-58 (2008).

Dated: November 15, 2013

s/Neil T. Bloomfield

Neil T. Bloomfield NC Bar Number 37800
Attorneys for Plaintiff

Moore & Van Allen PLLC
100 North Tryon Street
Suite 4700
Charlotte, NC 28202-4003
Telephone: +1-704-331-1084
Facsimile: +1-704-409-5660
Email: neilbloomfield@mvalaw.com

Of counsel:

Gabriel M. Ramsey (*pro hac vice*)
Orrick, Herrington & Sutcliffe LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401
Email: gramsey@orrick.com

Jeffrey L. Cox (*pro hac vice*)
Orrick, Herrington & Sutcliffe LLP
701 5th Avenue, Suite 5600
Seattle, WA 98104-7097
Telephone: (206) 839-4300
Facsimile: (206) 839-4301
Email: jcox@orrick.com

James M. Hsiao (*pro hac vice*)
Orrick, Herrington & Sutcliffe LLP
777 South Figueroa Street
Suite 3200
Los Angeles, CA 90017-5855
Telephone: (213) 612-2449
Facsimile: (213) 612-2499
Email: jhsiao@orrick.com

Attorneys for Plaintiff