Alvin Lee
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, New York, 10019
Telephone: (212) 506-5000

Gabriel Ramsey (*pro hac vice*)
Jeffrey L. Cox (*pro hac vice*)
Elena Garcia (*pro hac vice*)
ORRICK, HERRINGTON & SUTCLIFFE LLP
405 Howard Street
San Francisco, CA 94105-2669
Telephone: (415) 773-5700

Richard Domingues Boscovich (*of counsel*)
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Attorneys for Plaintiff
MICROSOFT CORPORATION

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MICROSOFT CORPORATION,

Plaintiff,

v.

JOHN DOES 1-5, CONTROLLING COMPUTER BOTNETS AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS,

Defendants.

Case No. 15-cv-6565-NGG-LB

MEMORANDUM OF LAW IN SUPPORT OF MOTION FOR DEFAULT JUDGMENT AND PERMANENT INJUNCTION

Plaintiff MICROSOFT CORPORATION ("Microsoft"), respectfully moves the Court to grant default judgment and issue a permanent injunction against Defendants John Does 1-5 ("Defendants"), who operated and controlled the Dorkbot botnets from and through the Internet domain names identified in Appendix A to the Proposed Order, filed herewith. Microsoft seeks 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 Dorkbot botnets, and (2) permanently transferring ownership of malicious domains identified in the Court's preliminary injunction order to Microsoft.

Default judgment is warranted here. Microsoft duly served Defendants with the Complaint, summons and all key pleadings in this action in a manner consistent with Due Process and this Court's instructions. Microsoft served Defendants by email on December 3, 4, 9, and 15, 2015, and publication beginning December 3, 2015. Additionally, after Microsoft executed this Court's TRO on December 3, 2015, Defendants quickly and purposefully reacted by activating previously dormant command and control domains so that they could continue to illegally control the Dorkbot infected devices. Declaration of Gabriel M. Ramsey In Support Of Motion for Default Judgment and Permanent Injunction ("Ramsey Decl.") ¶ 7. Between December 4-29, 2015 Defendants continued to route Dorkbot infected devices through other, previously dormant domains. *Id*. In spite of the notice, obvious impact on Defendants' illegal operations and wide publicity concerning this case, Defendants have failed to respond to this action. Defendants instead focused their efforts on resuming their fraudulent and criminal operations. *Id*.

The record establishes the elements of each of Microsoft's claims and also establishes the need for injunctive relief. Defendants received notice, but despite this, more than a year

after Microsoft filed suit, they still have not responded or otherwise appeared in this action. Accordingly, on December 2, 2016, the Clerk of the Court entered default against them. *See* Civil Docket For Case #: 1:15-cv-6565-NGG-LB, entry of December 2, 2016.

The issuance of a permanent injunction is also warranted. This injunctive relief is required to prevent further harm to Microsoft and the general public that would be caused if Defendants retake control of the Dorkbot infrastructure. Issues of substantial public importance weigh heavily in favor of a permanent injunction, as lifting the injunction on the botnet infrastructure will allow the Dorkbot botnets to resume their fraudulent and criminal operations. A permanent injunction is the only way to afford relief and abate future harm in this case, particularly given that, in the absence of such relief, the command and control domains would revert to the Defendants who would be able to misuse and intrude upon Microsoft's customers' computing devices and Microsoft's Windows operating systems.

There is no money at issue in granting a permanent injunction. There are no disputed material issues of fact; Microsoft presented overwhelming evidence of Defendants' fraudulent acts, which was set forth in detail in the Complaint and submitted at the time it filed the Complaint (Dkt. No. 1), 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 more than a year. Microsoft will be prejudiced by delay, as further discovery or progress in the case is precluded by Defendants' refusal to appear. Moreover, 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. Finally, 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.

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

I. STATEMENT OF FACTS

A. Procedural History

On November 23, 2015, Microsoft filed this suit, alleging that Defendants controlled a worldwide, illegal computer network, collectively known as the Dorkbot botnet, comprised of end-user computing devices connected to the Internet that Defendants had infected with malicious software. *See* Dkt. No. 1. Through various fraudulent techniques such as inserting malicious links into legitimate messages, innocent computing device users were lured to websites from which malicious Dorkbot botnet code is surreptitiously installed on their computers. Dkt. No. 9, ¶¶ 56-57. The botnet code then makes unauthorized changes to the infected computing devices and operating systems to bring the computing device under the control of the botnet operators—the Defendants in this case. Dkt. No. 1, ¶39. The Defendants then monitor the user's Internet browser communications and intercepts communications with various websites to steal user names and passwords. Dkt. No. 9, ¶ 67.

Simultaneously with the filing of the Complaint, Microsoft applied *ex parte* for a TRO, Seizure Order, and Order to Show Cause re Preliminary Injunction. *See* Dkt. Nos. 8-11. The goal was to disable and seize the Dorkbot botnets' command and control server software, operating from and through the domain names at issue in the case. On November 23, 2015, the Court issued an *Ex Parte* Temporary Restraining Order, Seizure Order and Order to Show Cause

Re Preliminary Injunction ("the TRO"). Dkt. No. 12. On December 3, 2015, Microsoft executed the TRO, disabling the targeted Dorkbot botnet infrastructure. On December 8, 2015, the Court issued a Preliminary Injunction redirecting Dorkbot botnet control domains to Microsoft's secure servers during the pendency of this action. *See* Dkt. No. 18.

When it issued the Preliminary Injunction, the Court found good cause to permit service by alternative means pursuant to Rule 4(f)(3). *Id.* at 8. The Court has directed that, under the circumstances, appropriate means of service sufficient to satisfy Due Process include emails to email accounts associated with Dorkbot botnet control domains and publication on a publically available Internet website. *Id.* On December 10, 2015, the Court granted Microsoft the ability to pursue discovery in order to obtain further contact and identity information of Defendants. *See* Dkt. No. 21. Doe discovery is now complete. Because Defendants used fake contact information to set up the Dorkbot botnet control domains comprising the Dorkbot botnet command and control infrastructure, Defendants' true identities remain unknown. Ramsey Decl. ¶¶ 12, 20, 22.

B. Microsoft Served Defendants Via Email and Publication

The Court authorized service by email and publication on November 23, 2015. Dkt. No. 12, ¶ 15. On December 3, 2015, Microsoft served email addresses associated with Defendants' IP addresses and Internet domains. Ramsey Decl. ¶¶ 11-19. Microsoft also served Defendants by publication on December 3, 2015 at the publicly available website http://botnetlegalnotice.com/dorkbot/. *Id.* ¶ 10. Microsoft used an email tracking service to monitor whether service emails were received and read. *Id.* ¶ 19. A number of the known email addresses successfully received the service of process emails at that time. *Id.*

Given that the email addresses were the point of contact actually used by the Defendants to register the botnet domains and IP addresses, the email addresses are the only available point of contact with Defendants and are the point of contact most likely to reach them. The time for Defendants to answer or respond to the complaint expired 21 days after service of the summons—at the latest, on December 28, 2015 (21 days after email service).

C. Microsoft's Doe Discovery Efforts

For over four months after serving Defendants, Microsoft attempted to obtain additional information regarding Defendants' identities to execute personal service. Microsoft has issued 12 subpoenas to domain registrars, email providers, Internet service providers ("ISP"), and other third party service providers in an effort to obtain additional information regarding Defendants' identities. *Id.* ¶¶ 21-33. Microsoft issued a first wave of subpoenas based on information used to obtain the registered domains. Based on information obtained from Microsoft's first wave of subpoenas, Microsoft sent additional subpoenas. However, the subpoena responses revealed that when registering for a domain or a free email address, Defendants were able to sign up using fictitious names. *Id.* ¶ 26.

In two instances, Defendants purchased domains through a registrar in the Russian Federation. Local counsel in the Russian Federation sent a request to these registrars asking for identifying information of Defendants. *Id.* ¶ 33. However, the registrars' response showed that Defendants used false names and incomplete or false addresses to purchase the domains. *Id.* Additionally, the login IP addresses used to log-in to email accounts were from disparate locations all over the world. *Id.* ¶ 28. Thus, Defendants were able to conceal their identities and physical locations.

Microsoft has used all reasonably available formal and informal means to investigate the true identities of the Defendants. *Id.* ¶ 34. Microsoft has exhausted its ability to investigate Defendants' true identities using civil discovery tools, despite their best efforts and the exercise of reasonable diligence to determine Defendants' identities. *Id.*

D. Injunctive Relief

The Court made several factual findings in the course of issuing preliminary injunctive relief to Microsoft. Among other findings, the Court concluded that:

- The Court has jurisdiction;
- Defendants have used the IP addresses and domains identified by Microsoft to control a malicious computer botnet;
- Unless enjoined, Defendants are likely to engage in conduct that violates the Lanham Act, CFAA, ECPA, RICO, and the common law doctrines of trespass to chattels, conversion, and unjust enrichment; and
- Defendants' conduct causes irreparable harm.

Dkt. No. 18, ¶¶ 1-13. Based on these findings, the Court enjoined Defendants from further violations of law and ordered U.S. domain registries to cause domains registered by Defendants to redirect to Microsoft secure severs.

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 botnets. Microsoft sets forth detailed evidence establishing this fact in the Complaint and in Microsoft's motion for the TRO. *See* Dkt. Nos. 1, 8-11. All such factual material is incorporated by reference, in support of this motion. The Court's order was extremely effective in disrupting the Dorkbot botnet. By disabling the command and control servers, the Court's TRO crippled Defendants' command and control infrastructure.

The permanent injunction sought by Microsoft directs that the Defendants cease their malicious conduct, and directs that the domains constituting the crucial infrastructure of the Dorkbot botnets remain under Microsoft's control. This will ensure that the Dorkbot operators will not be able to control or operate the botnets for malicious purposes.

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

A. Default Judgment Is Appropriate

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 entered default against the Defendants on December 2, 2016. Entry of a default judgment and permanent injunction against Defendants is now appropriate.

1. 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).

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 non-existent. Microsoft seeks injunctive relief prohibiting Defendants from operating the Dorkbot botnets or engaging in any of the malicious conduct alleged in this case. Microsoft also seeks injunctive relief directing the relevant domain registries to permanently transfer ownership to Microsoft of domains set forth in Appendix A of the proposed order submitted with this motion.

Second, this case presents a matter of substantial—even grave—public importance. Through operation of the Dorkbot botnets, Defendants have stolen online credentials and personal information from innocent computing device users. Dkt. No. 1, ¶¶ 27-28. In addition, Defendants specialize in providing access to the infected devices to other cybercriminals, the new cybercriminals download yet more malware onto the user's devices causing additional harm. Extending the protective measures put in place as part of the preliminary injunction is the only way to ensure, that the Dorkbot botnet operators do not quickly reconnect with the computing devices they had infected prior to this lawsuit and continue to defraud the owners or users of those computing devices.

Additionally, the possibility of a disputed issue regarding material facts is a remote one. Microsoft, in its detailed Complaint, pleadings and accompanying declarations has presented indisputable and overwhelming evidence that the domains at issue were used to control and propagate the Dorkbot botnet. *See* Dkt. Nos. 1, 8-11. Despite being served with the complaint more than a year ago, no Defendant 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 violated 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)); Electronic Communications Privacy A Computer Fraud and Abuse Act (18 U.S.C. § 1030); Electronic Communications Privacy Act (18 U.S.C. § 2701); the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); and the common law of unjust enrichment, trespass to chattels, and conversion. Dkt. No. 1, ¶¶46-101.

Third, Defendants' default is not merely technical. 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 were provided notice, and the evidence indicates that Defendants are actually or constructively aware of this action, but have chosen not to respond to Microsoft or the Court. Ramsey Decl. ¶¶ 21-33. As discussed above, Defendants have instead chosen to focus their efforts on resuming their fraudulent and criminal operations.

Fourth, Microsoft along with the other victims of the Dorkbot botnets, have 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 make their true

identities known to the Court or to Microsoft; have refused to engage in discovery or provide any manner of justification for their conduct; 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 a year after Microsoft filed the complaint, disabled their technical infrastructure, and launched extensive efforts to identify and serve them, Defendants have made no appearance in this case and have made no response whatsoever. Defendants are abusers of the Internet whose personal identities and physical locations remain unknown. 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. In the face of these difficulties, Microsoft went to extraordinary lengths to provide notice of this lawsuit to Defendants, but Defendants' failure to respond clearly establishes the grounds for default judgment. *Id*. ¶¶ 21-33.

Sixth, the effect of a default judgment will not be unduly harsh. No legitimate interests will be harmed. Microsoft seeks a permanent extension of the measures already protecting the public through the Courts preliminary injunction. These steps were crafted to disable the operation of the Dorkbot 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.

Seventh, Defendants' default is not the result of excusable neglect. 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 declaration in support of Microsoft's Motion for Default Judgment and Permanent Injunction. 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 warranted. 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 Microsoft and the U.S. public merely because they have been successful in using fake identities and addresses and operated the Dorkbot botnets from overseas.

2. Microsoft Has Sufficiently Plead Its Claims

Microsoft's Complaint sets forth in detail the legal and factual bases for the following statutory and common law claims.

a. 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. The Dorkbot botnet generates and uses unauthorized copies of Microsoft's trademarks in corrupted and sabotaged versions of the Windows operating system and Internet Explorer, MSN Messenger, and Windows Live Messenger software, including through the software operating from and through the Dorkbot command and control infrastructure. Dkt. No. 1, ¶¶ 58-61. By doing so, Defendants are likely to cause confusion, mistake, or deception as to the origin, sponsorship, or approval of the fake and unauthorized versions of the Windows operating system and Internet Explorer, MSN Messenger, and Windows Live Messenger software.

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).

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 Dorkbot Botnets' misleading and false uses of trademarks—including "Windows" and "Skype"—causes confusion and mistake as to Microsoft and its affiliation with the malicious conduct carried out by the botnet. Dkt. No. 1, ¶¶ 58-61. 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).

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, once a computing device is infected, the Windows operating system, Internet Explorer browser, MSN Messenger, and Windows Live Messenger applications on that computing device cease to operate normally and are transformed into tools of deception, but they still bear Microsoft's trademarks. Customers who experience degraded performance of Microsoft's products may attribute such poor performance to Microsoft, causing extreme damage to Microsoft's brands and trademarks and the goodwill associated therewith. Dkt. No. 1, ¶¶ 40, 58-61. This is another clear violation of the Lanham Act.

b. Defendants' Computer Fraud And Abuse Act Violations

The CFAA penalizes a party that: (1) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage, 18 U.S.C. § 1030(a)(5)(C); or (2) 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 (3) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage to a protected computer, 18 U.S.C. § 1030(a)(5)(A). 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).

Microsoft's customers' servers are "protected computers" under the CFAA. Defendants knowingly and intentionally have accessed and continue to access these protected computers without authorization and knowingly have caused and continue to cause the transmission of programs, information, code and commands, resulting in damage to the protected computers, the software residing thereon, and Microsoft. The Dorkbot botnets intentionally access without

authorization Microsoft's customers' computers and damage Microsoft-owned and licensed software, including Windows, Internet Explorer, MSN Messenger, and Windows Live Messenger, by corrupting these programs' behavior and converting them to instruments of criminality. Dkt. No. 1, ¶¶ 46-51. Additionally, the Dorkbot botnets' malicious code, installed without authorization on infected computers, steals end-user's online credentials. *Id.*

Moreover, the Dorkbot 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 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). Accordingly, Microsoft has plead and established their Computer Fraud & Abuse Act claims.

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). Microsoft's licensed operating systems on end-user computers are facilities through which electronic communication services are provided. The Dorkbot botnets intentionally access without authorization Microsoft's customer's computing devices and damage Microsoft-owned and licensed software, including Windows, Internet Explorer, MSN Messenger, and

Windows Live Messenger, by corrupting these programs' behavior and converting them to instruments of criminality. Dkt. No. 1, ¶¶ 53-55. The Dorkbot botnets' malicious code, installed without authorization on infected computers, searches files, intercepts user communications to and from websites owned and operated by Microsoft, and steals end-user's online credentials and other information. 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). Thus, Microsoft has plead and established their Electronic Communication Privacy Act claim.

d. 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 Microsoft's resources, by installing software that interferes with Microsoft's licensed Windows operating system and customer computers. Defendants' actions in operating the Dorkbot botnet result in unauthorized access to Microsoft's Windows operating system and Internet Explorer, MSN

Messenger, and Windows Live Messenger software and services and the computing devices on which such programs and services run, and result in unauthorized intrusion into those devices and theft of information and account credentials. These activities injure the value of Microsoft's user's 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).

e. 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 Dorkbot botnets have benefited from Microsoft's trademarks, brand names, and goodwill by, among other things, using Microsoft's trademarks, brand names and goodwill to steal legitimate user credentials. Dkt. No. 1, ¶¶ 90-95. Defendants chose to commercialize the Dorkbot botnet by creating and selling a Dorkbot "crime kit." Dkt. No. 9, ¶ 5. The crime kit, available for sale on hacker forums, allows other cybercriminals to quickly configure their own Dorkbot botnets. Dkt. No. 9, ¶ 5. Defendants use a large number of Microsoft trademarks in advertising their illegal Dorkbot crime kit, including Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, Internet Explorer and MSN. (Dkt. No. 9, ¶ 84).

Microsoft devotes significant computing and human resources to combating infections by the Dorkbot botnet, helping customers determine whether or not their computing devices are infected, and cleaning infected devices. Dkt. No. 1, ¶ 41. These efforts by Microsoft have cost

it approximately one million dollars, and thus the Dorkbot botnet and malware exact a tangible economic toll on Microsoft. *Id.* Thus, it is certainly inequitable for Defendants controlling the Dorkbot Botnets to retain the benefits of using Microsoft's trademarks and selling the "crime kits." Accordingly, Microsoft has plead and established their unjust enrichment claim.

f. 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 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.

(1) Dorkbot 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 Dorkbot Enterprise has existed since at least 2010, when Dorkbot was noted to be one of the most prolifically spread malware infections among the many that are tracked by security experts. Dkt. No. 1, ¶ 34. The Dorkbot Enterprise has continuously and effectively carried out its purpose of developing and operating global credential stealing botnets ever since. *Id.* This shows the Dorkbot Enterprise's purpose and longevity.

Additionally, the shared common botnet code used in the operation of the Dorkbot botnets, in furtherance of common financial interests, demonstrate the purpose of the Dorkbot 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 Dorkbot botnet code and their use of the Dorkbot botnet system to steal and exploit customer credentials. Dkt. No. 1, ¶¶ 77-80.

(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 Dorkbot 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 Dorkbot Enterprise. These acts are continuing and will continue unless and until this Court enters the requested permanent injunction.

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 and other account login credentials through the Dorkbot botnet system created and operated by Defendants. Dkt.

No. 1, ¶¶ 26-27, 77 -79. As set forth in detail in the Complaint and Application for TRO, Defendants have used the Dorkbot botnet system to intrude upon the computers of Microsoft, its customers, and steal, intercept and obtain this access device information from thousands of individuals, and have then used these fraudulently obtained unauthorized access devices to sell Dorkbot crime kits. Defendants have collected thousands of dollars from the illegal use or sale of legitimate user credentials in violation of 18 U.S.C. § 1029(a)(2).[1]

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

Defendants' botnets have carried out such massive theft by infecting more than a hundred thousand of computing devices running Microsoft's Windows operating system with its malicious software. As a direct result of Defendants' conduct, Microsoft has been forced to expend resources to clean infected systems running Microsoft software, mitigate the impact to customers, and investigate the source. Dkt. No. 1, ¶ 41. These efforts by Microsoft have cost it approximately one million dollars, and thus the Dorkbot botnet and malware exact a tangible economic toll on Microsoft. *Id.* 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)).

B. 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

[1] 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).

the Dorkbot botnets. Extending the measures already imposed by the Court to redirect Dorkbot botnet control domains to Microsoft's secure servers is critical to preventing the revival and renewed operation of the botnets. Therefore, relief directing the relevant Internet service providers that the botnet domains should be kept under Microsoft's control is the only way to effectively cure the harms complained of in this action. If the botnet domains are not kept offline or under Microsoft's control, Defendants could regain access to them and use them to revive the Dorkbot 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, ¶¶ 37-38.

Issuance of the requested permanent injunction is appropriate in this case because the traditional four-factor test for granting a permanent injunction is satisfied. A plaintiff must demonstrate: (1) that it has suffered an irreparable injury; (2) that remedies available at law, such as monetary damages, are inadequate to compensate for that injury; (3) that, considering the balance of hardships between the plaintiff and defendant, a remedy in equity is warranted; and (4) that the public interest would not be disserved by a permanent injunction. *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, Microsoft has suffered an irreparable injury through the unauthorized intrusion into their operating system installed on customer computers, the infringement and dilution of their trademarks by theft of customers' financial account credentials. *See* Dkt. No. 1, ¶¶ 95, 101. Second, Microsoft's injury cannot be compensated adequately by remedies at law – monetary damages would be inadequate to compensate Microsoft if Defendants were able to revive the Dorkbot botnets. Third, the balance of hardships tips

sharply in Microsoft's favor – Defendants were not using the relevant botnet domains for any legitimate purpose, but Microsoft would have to expend significant resources to filter and remediate the effects of increased illegal activity if the Dorkbot botnets were revived. Dkt. No. 1, ¶ 41. Finally the public interest would undoubtedly be served by ensuring that the Dorkbot botnets are not revived – the botnets took over end-users' computers and used them to steal account credentials. *Id.* ¶ 35.

Moreover, 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 the relief already imposed. No additional steps are needed. Federal courts 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 Stabil*e, 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). The use of the All-Writs Act in this case would be a narrow application, for limited relief. Microsoft merely seeks that domain registries redirect domains to Microsoft secure servers, a capability which the domain registries already use and have employed in the past.[2] Here, the assistance of the third party registries is necessary to ensure that

[2] *See Microsoft v. John Does 1-27*, Case No. 1:10-cv-00156 (E.D. Va. 2010) (Brinkema, J.), Dkt. No. 91 (order granting default judgment and permanent injunction) (granted limited relied ordering that VeriSign transfer registration of botnet domains to Microsoft); *Microsoft v. John Does, 1-11*, Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.), Dkt. No. 68 (order granting default judgment and permanent injunction) (ordered domain registries to maintain botnet domains in a disabled state for 24 months); *Microsoft v. John Does 1-82 et al.*, Case No. 3:13-CV-00319-GCM (W.D.N.C. 2013) (Mullen, J.), Dkt. No. 22 (order granting default judgment and permanent injunction) (granted permanent injunction ordering that domain registries transfer registration of botnet domains to

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.

C. Defendants' Actions Were Sufficiently Definite To Tie Them To Microsoft's 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 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.

Microsoft); *Microsoft et al. v. John Does 1-8*, Case No. 1-14-CV-811-LOG/TCB (E.D. Va. 2014) (O'Grady, J.), Dkt. No. 59 (order granting default judgment and permanent injunction) (granted permanent injunction ordering that domain registries transfer ownership and control of botnet domains to Microsoft).

Microsoft has presented considerable evidence to show that the domain names identified in this action were used to control, operate and propagate the Dorkbot botnets. As detailed in Microsoft's Request for Certificate of Default, service of process was directed at the nicknames, names and contact information specifically associated with the botnet domains. Dkt. No 23. Even though the Defendants' "real" names and physical locations are unknown, their actions are sufficiently definite to tie them to the operation of the Dorkbot botnets. Defendants leased domains through which the botnet was controlled. They supplied false names, fake addresses, 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 or registries to complain about their domains being disabled. Instead Defendants reacted by activating previously dormant command and control domains so that they could continue to illegally control the Dorkbot infected devices. Given the role those domains played in the operation and propagation of the Dorkbot 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 Microsoft and a permanent injunction against Defendants is 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 botnet domains at issue continue to be directed to Microsoft's secure servers.

Dated: December 8, 2016 Respectfully submitted,

By: /Alvin Lee/

ALVIN LEE
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, New York, 10019
Telephone: 212-506-5000
alee@orrick.com

GABRIEL M. RAMSEY (*pro hac vice*)
JEFFREY L. COX (*pro hac vice*)
ELENA GARCIA (*pro hac vice*)
ORRICK, HERRINGTON & SUTCLIFFE LLP
The Orrick Building
405 Howard Street
San Francisco, California 94105-2669
Telephone: 415-773-5700
gramsey@orrick.com
jcox@orrick.com
egarcia@orrick.com

RICHARD DOMINGUES BOSCOVICH (*of counsel*)
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399
Telephone: 425-704-0867
rbosco@microsoft.com

Attorneys for Plaintiff
Microsoft Corporation