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

MICROSOFT CORPORATION, a Washington corporation, Plaintiff, v. MARAT MAZYNSKIJ, an individual, and DMITRY CHUPAKHIN (AKA "SERGEY SKOROVOD"), an individual, Defendants.	Civil Action No: 1:13cv139 (LMB/TCB)

BRIEF IN SUPPORT OF MICROSOFT'S 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 Dmitry Chupakhin, who operated and controlled the Bamital botnet from and through the Internet domain and subdomain names identified in Appendix A to the Proposed Order, filed herewith.

The Bamital botnet has infected a very large number of Internet users' computers. (Amended Complaint, Dkt. No. 50, ¶¶36-54) 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.*, ¶ 40) The botnet code then waits for the unsuspecting user to attempt to carry out internet searches and, when they do so, takes control of the browser and Internet browser and forces the user to websites other than those intended. The botnet may also simply create invisible browser instances, unbeknownst to users, which generate fraudulent "clicks." These activities are then monetized by the generation of paid "traffic" through the online advertising ecosystem. (*Id.* ¶¶40-54)

Default judgment is warranted here. Microsoft served Defendant Dmitry Chupakhin with

its Amended Complaint and summons and related materials through personal and registered delivery, pursuant to Fed. R. Civ. P. 4(f)(2)(C)(i) and 4(f)(2)(A). Microsoft also served Defendant by email and publication, which are Court-ordered methods pursuant to Fed. R. Civ. P. 4(f)(3). On October 18, 2013, the Clerk of Court entered default against Defendant Dmitry Chupakhin. (Dkt. No. 59)

Pursuant to Fed. R. Civ. P. 55(b)(2), Microsoft seeks default judgment and a permanent injunction against Defendant Dmitry Chupakhin (1) prohibiting Defendant from operating or propagating the Bamital botnet, and (2) transferring ownership and control of the botnet command and control domains and subdomains 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 Amended Complaint (Dkt. No. 50), and Defendant Dmitry Chupakhin has not come forward to challenge this evidence in the Amended Complaint, or otherwise. The default is not technical or the result of excusable negligence, and the grounds for default are clearly established, as Dmitry Chupakhin has not responded to the Amended Complaint in any way for over three months, despite repeated personal service and repeated email communications directed to him. Microsoft will be prejudiced unless default judgment and a permanent injunction are issued, given that in the absence of such relief the botnet will be able to continue to injure Microsoft and its customers. 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, registrars and subdomain providers is needed to effect final relief against Defendant Dmitry Chupakhin, 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

On January 31, 2013, Microsoft filed this suit, alleging that defendants controlled a worldwide, illegal computer network, collectively known as the Bamital botnet, comprised of end-user computers connected to the Internet that had been infected with malicious software. (Dkt. No. 1) On June 19, 2013, Microsoft filed the Amended Complaint naming Mr. Chupakhin as a defendant responsible for these activities. (Dkt. No. 50) Through various fraudulent techniques, innocent computer users are lured to websites from which malicious botnet code is surreptitiously installed on their computers. (Dkt. No. 50, ¶¶ 40-54) 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.*) The botnet code then waits for the unsuspecting user to attempt to carry out internet searches and, when they do so, takes control of the Internet browser and forces the user to websites other than those intended by the user. The botnet may also simply create invisible browser instances—unbeknownst to the user—which generate fraudulent "clicks." These activities are then monetized by the generation and sale of Internet "traffic" through the online advertising ecosystem. (*Id*. ¶¶40-54)

Microsoft alleged that these acts violated the Computer Fraud and Abuse Act (18 U.S.C. § 1030); violated the Electronic Communications Privacy Act (18 U.S.C. § 2701); constituted 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)) and trademark dilution under the Lanham Act (15 U.S.C. § 1125(c)), and violated the common law of unjust enrichment, trespass to chattels, and conversion. (*Id*. ¶¶ 55-111) Microsoft sought injunctive and other equitable relief against Defendant Dmitry Chupakhin for his creation, control, maintenance, and ongoing use of the Bamital botnet, which has caused irreparable injury to Microsoft, Microsoft's customers, and the

general public. (*Id*. pp. 24-25) Simultaneously with the filing of the original complaint, Microsoft applied for a temporary restraining order and preliminary injunction. (Dkt. Nos. 3-9) The aim of this was to disable and seize the Bamital botnet's command and control server software, operating from and through the domain and subdomain names at issue in the case.

On January 31, 2013, the Court issued a temporary restraining order ("TRO"). (Dkt. No. 23) On February 7, 2013, Microsoft executed the TRO, disabling the targeted Bamital botnet infrastructure. (Dkt. No. 27) On February 13, 2013, the Court issued a preliminary injunction disabling, during the pendency of this action, the domains through which the Defendant operated and controlled the Bamital botnet. (Dkt. No. 38)

When it issued the temporary restraining order and preliminary injunction, the Court found good cause to permit service of the complaint and summons by alternative means pursuant to Rule 4(f)(3). (Dkt. No. 23, 38). Defendant Dmitry Chupakhin was duly served with a copy of the Amended Complaint and summons in the above-entitled action: (1) on July 8, 2013 by registered delivery requiring Mr. Chupakhin's signature, via international courier, (2) on August 26, 2013 by registered delivery requiring Mr. Chupakhin's signature, via the Russian Post and (3) on August 19 and 23 by email and publication.

Despite being served the Amended Complaint, summons and other pleadings in the action over the course of many months, Defendant Dmitry Chupakhin has not responded to the complaint or appeared in the action. Accordingly, on October 18, 2013, the Clerk of Court entered default against him (Dkt. No. 59).

B. Enjoining Defendant's Illegal Activities And Transferring The Botnet Domain And Subdomain Names To Microsoft Will Prevent The Harm Caused By The Botnet

The Internet domain and subdomain 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 Defendant used to control the Bamital botnet. (*See* Dkt. No. 50, p. 1) Microsoft set forth detailed evidence establishing this fact in the Amended Complaint and in connection with Microsoft's motion for the TRO. (*See* Dkt. Nos. 50 and 3-9) All such factual material is

incorporated by reference, in support of this motion.

The permanent injunction sought by Microsoft directs that Defendant Dmitry Chupakhin cease his malicious conduct, and directs that the domains and subdomains constituting the infrastructure of the Bamital botnet be transferred to Microsoft's ownership and control. This will ensure that the Bamital botnet will not be able to continue its 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 DEFENDANT DMITRY CHUPAKHIN

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 Defendant Dmitry Chupakhin. Entry of a default judgment and permanent injunction against Dmitry Chupakhin is now appropriate.

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

The grant of default judgment is committed to the discretion of the court. *Park Corp. v. Lexington Ins. Co.,* 812 F.2d 894, 896 (4th Cir. 1987); *EMI April Music, Inc. v. White,* 618 F. Supp. 2d 497, 506 (E.D. Va. 2009). 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.* (citing Wright, Miller & Kane, Federal Practice and Procedure: Civil 3d § 2685); *see also Tweedy v. RCAM Title Loans, LLC,* 611 F. Supp. 2d 603, 606 (W.D. Va. 2009). Finally, a court, in granting default judgment, must determine whether the well-pleaded allegations in the complaint support the relief sought. *Ryan v. Homecomings Fin. Network*, 253 F.3d 778, 780-781 (4th. Cir. 2001).

In this case, these factors weigh heavily in favor of granting default judgment and entering a permanent injunction against Defendant. 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 Dmitry Chupakhin from operating the Bamital botnet or engaging in any of the malicious conduct alleged in this case. Microsoft also seeks injunctive relief directing the relevant domain registries, registrars and subdomain providers to transfer to Microsoft ownership and control of the domains and subdomains used to control and propagate the Bamital botnet, so that the botnet cannot be revived through those domains and subdomains.

Second, this case presents a matter of serious public importance. Through operation of the Bamital botnet, Defendant has taken control of a large number of victim computers, has taken control of those users' Microsoft Windows operating system, Internet Explorer browser and Bing search engine results, has "hijacked" the functionality of that software and forced users' computers to visit websites without the users' consent and has monetized this activity through fraud carried out in the online advertising ecosystem. (Dkt. No. 50, ¶¶ 36-54) By these actions, Defendant has 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 and subdomains to Microsoft will help ensure that the Bamital botnet does 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 Amended Complaint, pleadings and accompanying declarations have adduced incontrovertible and overwhelming evidence that the domains and subdomains at issue were used to control and propagate the Bamital botnet. (*See* Dkt. Nos. 50, 3-9) Despite being served, Defendant Dmitry Chupakhin has not appeared or otherwise attempted to dispute any issue of fact or law in this case. The allegations and evidence in the detailed Amended Complaint and otherwise in the record establishes that the operation of the Bamital botnet violated the Computer Fraud and Abuse Act (18 U.S.C. § 1030); Electronic Communications Privacy Act (18 U.S.C. § 2701); the Lanham Act (15 U.S.C. § 1114 and § 1125(a) and (c)); and the common law of unjust enrichment, trespass to chattels, and conversion. (*See* Dkt. No. 50, ¶¶ 55-111)

Third, Defendant's default is not merely technical. This is not a situation where Defendant has merely missed a deadline by a few days. Rather, Defendant has 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 Dmitry Chupakhin has been provided notice and the opportunity to appear, and the evidence indicates that Defendant is actually aware of this action, but has chosen not to respond. (*See* Dkt. No. 57-59)

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

Fifth, the grounds for default are clearly established. Even eight 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 Defendant Dmitry Chupakhin, he has made no appearance in this case and has made no response whatsoever to the original complaint or the Amended Complaint. Microsoft went to extraordinary lengths to provide notice of this lawsuit to Defendant Dmitry Chupakhin, and certain of the original defendants did ultimately respond to Microsoft's service of process, proving its sufficiency. Dmitry

Chupakhin's 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 and subdomains, effectively continuing the measures already protecting the public through the Court's preliminary injunction. The current control exerted over the Bamital botnet domains and subdomains disable the operation of the Bamital botnet while causing the least amount of burden on third party domain registries, registrars and subdomains providers responsible for administering those domains and subdomains.

Seventh, Defendant Dmitry Chupakhin's default is not the result of excusable neglect. Microsoft went to extraordinary lengths to provide notice of this lawsuit to him. (*See* Dkt. Nos. 57-58) It is quite evident that Dmitry Chupakhin received ample notice of the action against him and has 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 Dmitry Chupakhin has adopted a strategy of "laying low" while this lawsuit is pending, after which period he hopes to resume his illegal acts.

Given the significant factual substance and authority submitted in the Amended 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 Defendant Dmitry Chupakhin. Defendant, who has 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 he has been successful in operating the Bamital botnet from overseas.

1. Microsoft Has Sufficiently Pled Its Claims

Microsoft's Amended Complaint sets forth in detail the legal and factual bases for the following statutory and common law claims: (1) violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030), (2) violations of the Electronic Communications Privacy Act (18 U.S.C. § 2701); (3) trademark infringement under the Lanham Act (15 U.S.C. § 1114); (4) false

designation of origin under the Lanham Act (15 U.S.C. § 1125(a)); (5) trademark dilution under the Lanham Act (15 U.S.C. 1125(c)), (6) unjust enrichment; (7) trespass to chattels / computer trespass, and (8) conversion.

a. 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 the computers of their customers are "protected computers" under the CFAA. Defendant intentionally accessed Microsoft's servers, Microsoft's proprietary operating system, Internet Explorer software and Bing search engine functionality, as well as Microsoft's customers' computers, without authorization, and burdened those computers by infecting them with malicious code and executing that code without consent. The Bamital botnet intentionally accesses without authorization Plaintiff Microsoft's Windows operating system and Internet Explorer software to "hijack" Bing search engine browser sessions, force Microsoft's customers to visit websites without their knowledge or consent and to force that software and those computers to invisibly generate a massive number of fraudulent "clicks" that Defendant then monetizes through fraud upon the online advertising ecosystem. Thereby, Defendant Dmitry Chupakhin has caused damage. (Dkt. No. 50, ¶¶ 24-54, 61-65)

The Bamital botnet's unauthorized access is precisely the type of activity the Computer Fraud and Abuse Act is designed to prevent. *See e.g. Global Policy Partners, LLC v. Yessin,* 2009 U.S. Dist. LEXIS 112472, *9-13 (E.D. Va. 2009) (accessing computer using credentials

[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).

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); *Physicians Interactive v. Lathian Sys., Inc.,* 2003 U.S. Dist. LEXIS 22868, *25 (E.D. Va. 2003) (CFAA violation where the defendant hacked into a computer and stole confidential information). Accordingly, Microsoft has pled and established its Computer Fraud & Abuse Act claims.

b. Electronic Communications Privacy Act Violations

The Electronic Communications Privacy Act prohibits "intentionally access[ing] without authorization a facility through which electronic communications are provided" or doing so in excess of authorization and, in doing so, obtaining, altering, or preventing authorized access to an electronic communication while it is in electronic storage. 18 U.S.C. § 2701(a). The search engine servers of Microsoft are facilities through which electronic communication services are provided. Microsoft's licensed Windows operating systems and Internet Explorer software on end-user computers, moreover, are facilities through which electronic communication services are provided. The Bamital botnet's malicious code, installed without authorization on infected computers, hijacks Internet browser and search sessions and intercepts user communications to and from servers and software of Microsoft, and uses that information to force users to visit fraudulent sites, without their consent, and to generate fraudulent "clicks" using their computers. Once the Bamital botnet software intercepts the user's search terms and search results, this information is used to redirect the user to fraudulent websites, in order to forcibly monetize that user's activity. (Dkt. No. 50, ¶¶ 24-54, 61-65) 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, *8-13 (E.D. Va. 2009) (unauthorized access to emails was actionable under ECPA); *State Analysis, Inc.*, 621 F. Supp. 2d at 317-318 (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 data stored on a third-party communication service provider'

system violated ECPA). Microsoft has pled and established its Electronic Communication Privacy Act claim.

c. 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. Defendant reproduces fraudulent versions of Microsoft's "Windows," "Internet Explorer" and "Bing" trademarks, in the adulterated versions of those software offerings that are created by the Bamital malware. These are registered, famous and distinctive trademarks, used in fraudulent versions of the software and used to deceive victims to believe that they are using legitimate versions of the software, despite the impaired functionality caused by the Bamital malware. This activity causes confusion and causes consumers and users to mistakenly associate Microsoft with the malicious activity of the Bamital botnet. Defendant's use of counterfeit trademarks in connection with such fraudulent schemes is likely to cause confusion and mistake and to deceive consumers. (Dkt. No. 50, ¶¶ 24-54, 66-74)

This is a clear violation of the Lanham Act § 1114. *See Otels, Inc. v. Altun*, 2012 U.S. Dist. LEXIS 114584, *9-12 (E.D. Va. 2012) (unauthorized use of a registered mark in an Internet use, which was likely to cause confusion among consumers, constituted a violation of § 1114); *see also Audi AG v. Shokan Coachworks, Inc.,* 592 F. Supp. 2d 246, 279 (N.D.N.Y. 2008) (use of the plaintiffs' marks in the defendants' email addresses created a likelihood of consumer confusion); *Kuklachev v. Gelfman,* 629 F. Supp. 2d 236, 258 (E.D.N.Y. 2008) (Lanham Act § 1114 violation for infringement of trademarks where confusion was likely to result from use of plaintiffs' name and images in connection with defendants' advertisements); *Brookfield Commc'ns. v. W. Coast Entm't Corp.*, 174 F.3d 1036, 1066-1067 (9th Cir. 1999) (Lanham Act §1114 for infringement of trademark in software and website code). It is obvious that confusion is likely, as the "Microsoft," "Windows," "Internet Explorer" and "Bing" brands are strong and Defendant's use of those marks in adulterated versions of the Windows operating system, Internet Explorer software and Bing browser functionality is intended and likely to confuse

consumers into believing that they are using authentic versions of these products—so that they will continue to use the adulterated software and be subject to the fraudulent click and search hijacking schemes. These factors indicate a likelihood of confusion. *Otels, Inc.*, 2012 U.S. Dist. LEXIS 114584 at *9-12.

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 Bamital botnet's misleading and false uses of trademarks—including "Microsoft," "Windows," "Internet Explorer" and "Bing," causes confusion and mistake as to Microsoft's affiliation with the malicious conduct carried out by the botnet. (Dkt. No. 50, ¶¶ 24-54, 75-82) This activity is a clear violation of Lanham Act § 1125(a). *See e.g. America Online v. IMS*, 24 F. Supp. 2d 548, 551-552 (E.D. Va. 1998) (spam email with purported "from" addresses including plaintiff's trademarks constituted false designation of origin); *see also 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, Defendant's misuse of Microsoft's famous marks in connection with malicious conduct aimed at Microsoft's customers and the public dilutes the famous marks by tarnishment and by blurring consumers' associations with the marks. (Dkt. No. 50, ¶¶ 24-54, 83-91) This is another clear violation of the Lanham Act. *See America Online*, 24 F. Supp. 2d at 552 (spam

email with purported "from" addresses including plaintiff's trademarks constituted dilution); *see also Hotmail Corp.*, 47 U.S.P.Q. 2d at 1024, 1025-26; (spam e-mail with purported "from" addresses including plaintiff's trademarks constituted dilution).

d. Trespass to Chattels/Conversion

A trespass to chattels occurs "when one party intentionally uses or intermeddles with personal property in rightful possession of another without authorization," and "if the chattel is impaired as to its condition, quality, or value." *America Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 451-452 (E.D. Va. 1998); *AOL v. IMS*, 24 F. Supp. 2d 548 (*citing Vines v. Branch*, 244 Va. 185, 418 S.E. 2d 890, 894 (1992)) (trespass to chattels actionable in Virginia); *see also Barr v. City of Roslyn*, 2010 U.S. Dist. LEXIS 5541, *6-7 (E.D. Wash. 2010) (same). Similarly, "[a] person is liable for conversion for the wrongful exercise or assumption of authority over another's goods, depriving the owner of their possession, or any act of dominion wrongfully exerted over property in denial of, or inconsistent with, the owner's rights." *James River Mgmt. Co. v. Kehoe*, 2009 U.S. Dist. LEXIS 107847, *22-23 (E.D. Va. 2009); *Barr*, 2010 U.S. Dist. LEXIS 5541 at *6-7 (under Washington law "conversion is the act of willfully interfering with any personal property without lawful justification, which causes the person entitled to possession to be deprived of that possession")

The unauthorized installation of software onto and subsequent control over Microsoft's licensed Windows operating system software, Internet Explorer software and Bing search engine web page, and computers of customers interferes with and causes injury to the value of those properties. (Dkt. No. 50, ¶¶ 24-54, 92-97, 108-111) Thus, this conduct is an illegal trespass and also constitutes conversion. *See Physicians Interactive v. Lathian Sys.*, 2003 U.S. Dist. LEXIS 22868 (E.D. Va. 2003) (granting TRO and preliminary injunction where defendant hacked computers and obtained proprietary information holding "there is a likelihood that the two alleged attacks that [Plaintiff] traced to Defendants were designed to intermeddle with personal property in the rightful possession of Plaintiff."); *In re Marriage of Langham*, 153 Wn.2d 553, 566 (Wash. 2005) (conversion of intangible property); *Kremen v. Cohen*, 337 F.3d 1024, 1034 (9th Cir. Cal. 2003) (recognizing that hacking into a computer system and injuring

data supports a conversion claim); *see also State v. Riley*, 121 Wn. 2d 22, 32 (Wash. 1993) (affirming conviction for "computer trespass" under Washington law for defendant's "hacking activity").

Likewise, unauthorized intrusion into Microsoft's Bing Ads servers by directing fraudulent clicks to that service injures Microsoft's property and constitutes a trespass. *See e.g. America Online, Inc. v. IMS*, 24 F. Supp. 2d 548, 550 (E.D. Va. 1998) (senders of spam e-mail committed trespass when they "caused contact with [plaintiff's] computer network ... and ... injured [plaintiff's] business goodwill and diminished the value of its possessory interest in its computer network."); *State v. Heckel*, 143 Wn. 2d 824, 834 (Wash. 2001) (spam e-mail burdens possessory interest in computers; recognizing trespass to chattels, citing *AOL v. IMS*);

e. Unjust Enrichment

The elements of a claim of unjust enrichment are (1) the plaintiff's conferring of a benefit on the defendant, (2) the defendant's knowledge of the conferring of the benefit, and (3) the defendant's acceptance or retention of the benefit under circumstances that "render it inequitable for the defendant to retain the benefit without paying for its value." *Nossen v. Hoy,* 750 F. Supp. 740, 744-45 (E.D. Va. 1990) (Virginia law); *Ballie Commc'ns Ltd. v. Trend Bus. Sys. Inc.,* 61 Wn.App. 151, 160, 810 P.2d 12 (1991) (same, under Washington law).

Here, without authorization, the Defendant has taken the benefit of Microsoft's servers, networks, its licensed Windows operating system software, its Internet Explorer browser and Bing search engine, and the computers of Microsoft's customers. Defendant has done so by improperly infecting these computers, and causing them to hijack users' Internet Explorer web browser sessions and Bing search engine results to engage in click-fraud. (Dkt. No. 50, ¶¶ 24-54, 98-107). Defendant has profited from this activity, including by attempting to direct fraudulent traffic to Microsoft's Bing Ads platform. (*See id.*) Thus, it is certainly inequitable for Defendant to retain this benefit. Microsoft is likely to succeed on the merits.

III. CONCLUSION

For all of the foregoing reasons, entry of default judgment and a permanent injunction in

favor of Microsoft and against Defendant Dmitry Chupakhin are appropriate. Microsoft respectfully requests entry of default judgment against Defendant Dmitry Chupakhin and a permanent injunction prohibiting Dmitry Chupakhin from engaging in the conduct underlying this case and directing that the ownership and control of the botnet domains and subdomains at issue be transferred to Microsoft.

Dated: October 24, 2013 Respectfully submitted,

ORRICK, HERRINGTON & SUTCLIFFE LLP

/s/ Lauren Parker

LAUREN PARKER
Va. State Bar No. 77018
Attorneys for Plaintiff Microsoft Corp.
ORRICK, HERRINGTON & SUTCLIFFE LLP
Columbia Center
1152 15th Street, N.W.
Washington, D.C. 20005-1706
Telephone: (202) 339-8400
Facsimile: (202) 339-8500
lparker@orrick.com

Of counsel:

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

JEFFREY L. COX (*pro hac vice*)
Attorney for Plaintiff Microsoft Corp.
ORRICK, HERRINGTON & SUTCLIFFE LLP
701 5th Avenue, Suite 5600
Seattle, WA 98104-7097
Telephone: (206) 839-4300
Facsimile: (206) 839-4301
jcox@orrick.com

CERTIFICATE OF SERVICE

I hereby certify that the 24th day of October, 2013, I will electronically file the foregoing with the Clerk of the Court using the CM/ECF system. Copies of the foregoing were also served on the defendant listed below by registered international delivery and by electronic mail.

Dmitry Chupakhin aka "Sergey Skorovod"
Barbyusa St., Bldg. 134, Apt. 24
Chelyabinsk 454078
Russian Federation

Дмитрий Чупахин ("Сергей Скоровод")
ул. Барбюса , д. 134, кв. 24
Челябинск 454078
Российская Федерация

serg.skorovod@gmail.com
pizdato77@gmail.com
dmitry@chupahin.com
davidzonbigid@gmail.com
taxi.1979@mail.ru
trusart88@gmail.com
viktorhamov@yahoo.com
viktorhamov2@yahoo.com
todeallr@yahoo.com
auselloyosjuv@gmail.com
billsberryhok@gmail.com
peter1979@qmail.com
alexsmit2011@gmail.com
seven2011@gmail.com
rosannaleazuk@gmail.com
s15051575@yandex.ru
s15@mail.ru
tarosmit@yandex.ru
worldsearch@yandex.ru
martiula2@bk.ru

/s/ LAUREN PARKER

LAUREN PARKER
Va. State Bar No. 77018
Attorneys for Plaintiff Microsoft Corp.
ORRICK, HERRINGTON & SUTCLIFFE LLP
Columbia Center
1152 15th Street, N.W.
Washington, D.C. 20005-1706
Telephone: (202) 339-8400
Facsimile: (202) 339-8500
lparker@orrick.com