Randall D. Haimovici (*Pro Hac Vice Pending*)
rhaimovici@shb.com
Rachael M. Smith (*Pro Hac Vice Pending*)
rxsmith@shb.com
SHOOK, HARDY & BACON L.L.P.
One Montgomery, Suite 2700
San Francisco, California 94104-4505
Telephone: 415.544.1900
Facsimile: 415.391.0281

Tony M. Diab (Nevada State Bar No. 12954)
tdiab@shb.com
SHOOK, HARDY & BACON L.L.P.
5 Park Plaza, Suite 1600
Irvine, California 92614-2546
Telephone: 949.475.1500
Facsimile: 949.475.0016

Robert J.B. Flummerfelt (Nevada State Bar No. 11122)
rflummerfelt@hotmail.com
Rami Hernandez (Nevada State Bar No. 13146)
rhernandeznsj@hotmail.com
CANON LAW SERVICES, LLC
7251 W. Lake Mead Blvd., Suite 300
Las Vegas, Nevada 89128
Telephone: 702.562.4144
Facsimile: 702.866.9868

Attorneys for Plaintiff
MICROSOFT CORPORATION

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

MICROSOFT CORPORATION, Plaintiff, vs. NASER AL MUTAIRI, an individual; MOHAMED BENABDELLAH, an individual; VITALWERKS INTERNET SOLUTIONS, LLC, d/b/a NO-IP.com; and DOES 1-500, Defendants.	Case No. 14-cv-0987 **FILED UNDER SEAL** **BRIEF IN SUPPORT OF APPLICATION OF MICROSOFT CORPORATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE REGARDING PRELIMINARY INJUNCTION**

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

OTHER AUTHORITIES

INTRODUCTION

In early 2014, Microsoft investigated the top malware threats impacting its consumers. It found that a significant amount of malware was programmed to connect to Internet domains owned and leased by Defendant Vitalwerks (or No-IP). Further investigation revealed that No-IP is a major hub of malware activity and in particular, the Bladabindi/Jenxcus malware. Microsoft seeks this Temporary Restraining Order (TRO) to put a stop to the harm caused by this malware and requests an order that will allow it to block traffic between infected computers and malicious No-IP sub-domains, through which the Malware Defendants (Mutairi, Benabdellah, and Does 1-500) communicate with the infected computers.

An *ex parte* application for a TRO is warranted and necessary here. First, given the Malware Defendants' abusive conduct, which Defendant Vitalwerks enables through its Dynamic DNS service, Microsoft is likely to succeed on the merits of its computer-abuse and common law claims. Second, Defendants' conduct has caused Microsoft irreparable harm including the loss of goodwill, brand integrity, and resources expended to investigate and combat this abuse. And Microsoft is not the only one harmed–with the malware, Defendants are able to control user computers and steal sensitive information from unknowing and unsuspecting Microsoft customers and the public at large, causing them untold harm. Third, the balance of hardships weighs in Microsoft's favor. The Malware Defendants' criminal activities serve no legitimate purpose, and Microsoft only seeks to block traffic to the malicious sub-domains. Defendant Vitalwerks generates no known income from offering this free service. Thus, there is no hardship on Defendants or any third party. Fourth, the public interest is served by granting the TRO because the harm Defendants inflict on Microsoft and its customers also harms millions of other computer users and companies worldwide as well.

Additionally, *ex parte* relief is required here where advanced notice will permit Defendants, who exist and operate primarily in a virtual world, to disappear without a trace, thus rendering Microsoft's efforts fruitless. Advanced notice would further thwart Microsoft's efforts to stop this abuse because Defendants will destroy evidence necessary for Microsoft to prove its claims. If this Court grants the *ex parte* relief, Microsoft will provide notice of the hearing and serve all Defendants with the complaint and TRO by all means necessary.

STATEMENT OF FACTS

Vitalwerks's Free Dynamic DNS Service Is a Hub of Malware Activity

This case began as an investigation by Microsoft into the top malware threats impacting its customers. (Lyons Decl. ¶ 10.) To do this, Microsoft began to monitor data it was receiving from anti-malware utilities running on its consumers' computers. (*Id.*) When malware is detected, it sends data back to Microsoft, and from this data, Microsoft can identify the type of malware, whether it can be safely removed, and whether the malware is hard coded to communicate with other computers. (*Id.*) Microsoft determined from this investigation that a significant number of cases involved malware programmed to communicate with No-IP Internet sub-domains, owned and leased by Defendant Vitalwerks as part of its free Dynamic DNS service. (*Id.*)

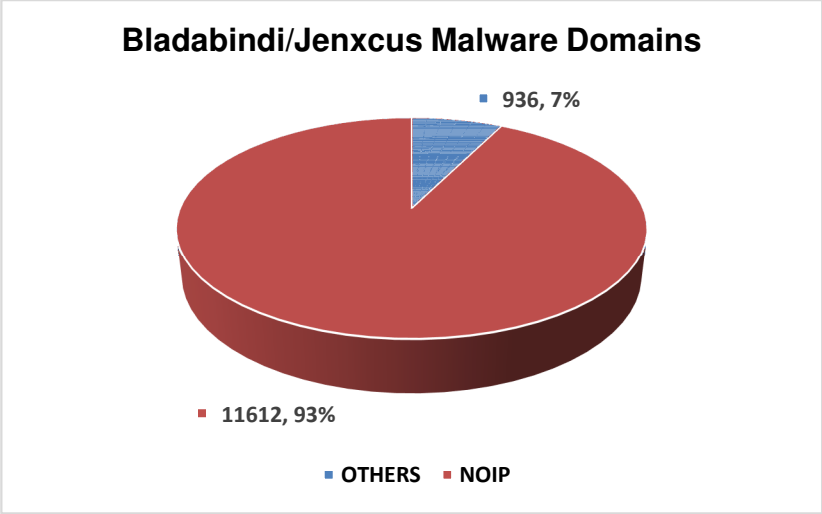
Further investigation showed that No-IP is functioning as a major hub for 245 varieties of malware circulating on the Internet. (*Id.* ¶ 11.) Through No-IP sub-domains, a very large number of small, transient websites are provided a continuous Internet presence. (*Id.* ¶ 12.) For example, malware on a person's infected computer might be programmed to contact "hacker-0005.no-ip.biz." (*Id.*) The person's computer would first contact no-ip.biz to get the address of the virus sub-domain, which has a dynamic IP address and is frequently changing. (*Id.*) No-ip.biz, however, would have the current IP address due to the Dynamic Update Client constantly updating No-IP's servers, and no-ip.biz would be able to direct the person's computer onward. (*Id.*) Thus, the Dynamic DNS system provides computers that move from IP address to IP address a stable domain name for malware infected computers to contact. (*Id.*) As long as that computer updates no-ip.biz as to its current IP address, malware infected machines attempting to reach it will always be able to do so. (*Id.*)

Dynamic DNS can be exploited to support and monetize cybercrime activities. This fact is evident from the massive number of malware supported by No-IP domains. By studying thousands of samples of malware, Microsoft has been able to identify approximately **18,472 sub-domains** of No-IP that used by malware distributors, and there are likely many more. (*Id.* ¶ 13.) Other Internet security researchers have observed the same. (*Id.*)

//

The Majority of Malware Using No-IP is Bladabindi/Jenxcus

By far, the majority of malware using No-IP domains is from the Bladabindi/Jenxcus family of malware. (Lyons Decl. ¶ 15.) Furthermore, as shown in the figure below, 93% of domains supporting Bladabindi/Jenxucs are No-IP domains. (*Id.*)



Defendant Mutairi is the creator and owner of Bladabindi. (Tan Seng Decl. ¶ 7.) Defendant Benabdellah created a variant of the Jenxcus malware that is closely related in function to Bladabindi. (*Id.*) Bladabindi/Jenxcus malware can be downloaded by other cybercriminals who then can use the malware's "dashboard" created by Defendant Mutairi to customize the malware to suit their needs. (*Id.* ¶ 21.) The dashboard is a user interface that allows the user to customize the malware and control the infected computers. (*Id.*) Microsoft has detected over 7,486,833 instances of Windows computers that have encountered one or more versions of Bladabindi or Jenxcus malware in the past year. (*Id.* ¶ 28.) This likely represents only a small subset of the number of computers because Microsoft is only able to monitor machines running its anti-malware software. (*Id.*) Based on market share data, the total number of detections over the past year may easily be two to three times this amount. (*Id.*)

Bladabindi/Jenxcus Infected Computers Become Part of a Botnet

When a computer is infected with Bladabindi or Jenxcus, it becomes part of a "botnet." (Lyons Decl. ¶ 16.) A botnet is a collection of individual computers, each running malware that allows communications between the infected computers to one or more other computers controlled

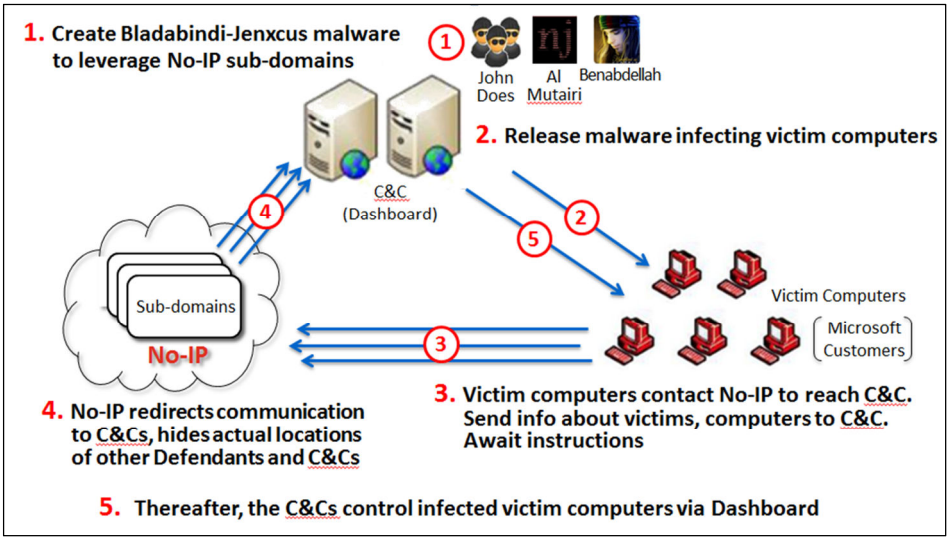
by the distributor of the malware, typically referred to as the "command and control." (*Id.*) Through the command-and-control computer or computers, cybercriminals are able to control the infected computer, steal information from the infected computer, and provide instructions or additional malware modules to the infected personal computers and upload data from them. (*Id.*) Cybercriminals often use botnets because of their ability to support a wide range of illegal conduct, their resilience against attempts to disable them, and their ability to conceal the identities of the malefactors controlling them. (*Id.*)

Microsoft has carefully studied the Bladanindi and Jenxcus botnet architecture, design, and functions. A Bladabindi/Jenxcus botnet consists of two tiers: the infection tier and the command-and-control tier. (Lyons Decl. ¶ 16.) The infection tier is comprised of infected personal computers owned by innocent and unsuspecting people. (*Id.*) These might be office or home desktop computers, laptop computers, computers in public libraries, and so forth. (*Id.*) Computers can become infected in one of several ways. A person may use an infected thumb-drive borrowed from a friend or colleague that contains the malware; access a malicious link or hacked website on which the malware downloader is staged; or download other malware containing instructions to download Bladabindi or Jenxcus. (Tan Seng Decl. ¶¶ 9-11.)

Once Bladabdindi/Jenxcus has been downloaded, the user still needs to access the malicious file for the malware to become active. Here, the malware tricks consumers into opening and running the file by disguising itself as a legitimate file. (*Id.* ¶ 12.) The malware uses deceptive file names and icons that are familiar to the user, such as "Facebook.exe," or that entice the user to open the file like "StartupFaster.exe" or "hot.exe." (*Id.*) Some Jenxcus variations will use the same name and icon as files already present on the user's thumb-drive. (*Id.*) When the malware is run, it will copy itself to a location on the user's computer that ensures that the malware will run every time the computer is started. (*Id.*)

Once the malware is activated, it will instruct the infected computer to contact the command-and-control computer (the second tier in the botnet) to let it know that the computer is ready to receive instructions from a Malware Defendant. (Lyons Decl. ¶ 18.) Malware Defendants program the malware to instruct the infected computer to reach out to a specific domain, which will resolve to

the IP address for the command-and-control computer, as depicted in the diagram below. (*Id.* ¶ 19; Tan Seng Decl. ¶ 25.)



Once the infected computer is directed to the command and control, the Malware Defendant can then directly communicate with the infected computer. (Lyons Decl. ¶ 20.) No-IP domains are part of the botnet infrastructure. Without No-IP domains, the infected computers would not be able to locate the Malware Defendants' command-and-control computers. (*Id.*; Tan Seng Decl. ¶ 19.)

Once the computer is infected with Bladabindi or Jenxcus, the Malware Defendants gain control over the consumers' computers, and they can conduct a variety of illegal and harmful activities, including accessing the user's files, turning on the computer's video camera or microphone to record victims, recording keystrokes to obtain sensitive information like passwords and credit card numbers, taking snapshots of the user's desktop, and sending commands to download additional malware. (Tan Seng Decl. ¶¶ 18, 21-23.)

Vitalwerks Is on Notice That Its Services Are Being Abused

The Internet security community has taken notice of the abuse occurring on No-IP's sub-domains. In April 2013, OpenDNS published an article online detailing its investigation into Dynamic DNS abuse, and it identified No-IP sub-domains as the most used for malicious intent of any other provider. (Haimovici Decl. ¶ 32 & Ex. 23.) No-IP published the following response, representing that the company had a strict abuse policy and an abuse team was "constantly working" to combat computer fraud and crimes:

> No-IP, we have a very strict abuse policy. Our abuse team is constantly working to keep our domains free of spam and malicious activity. Even with such precautions, our services do fall prey to cyberscammers and spammers. We highly encourage our users and others to let us know if they come across a hostname that isn't abiding by our Terms of Service. We dislike spammers and scammers just as much as everyone else. To report a violation of our TOS or any other abuses of our services, please email abuse@no-ip.com.

(*Id.* ¶ 33 & Ex. 23.) Despite its representation of having a "very strict abuse policy," the abuse on No-IP sub-domains continued.

Another Internet security group, Cisco, published an article on February 11, 2014 that again outlined the extensive abuse occurring on No-IP domains, including the distribution of malware. (Haimovici Decl. ¶ 34 & Ex. 24.) No-IP published a similar response and even provided that the company "work[s] with law enforcement daily to ensure that we are doing our part to keep the internet safe." (*Id.* ¶ 34 & Ex. 25.) Other Internet security firms have made similar reports. (Lyons Decl. ¶ 13.) Nonetheless, the extensive abuse of No-IP sub-domains continued. After the February Cisco report was published, Microsoft continues to see 2,000-3,000 new unique malware samples per month that are supported by No-IP. (*Id.*)

ARGUMENT

A TRO or preliminary injunction is warranted where the movant establishes (1) a likelihood of success on the merits; (2) that it is likely to suffer irreparable harm in the absence of preliminary relief; (3) that the balance of hardships tip in favor of granting the requested relief; and (4) that injunctive relief is in the public interest. *Dumas v. Gommerman*, 865 F.2d 1093, 1095 (9th Cir. 1989); *see also Cal. Indep. Sys. Operator Corp. v. Reliant Energy Servs., Inc.*, 181 F. Supp. 2d 1111, 1126 (E.D. Cal. 2011); *ViaView, Inc. v. Blue Mist Media*, 2012 WL 6007204, at *1-2 (D. Nev. Nov. 30, 2012). Microsoft has met these requirements here. Microsoft has also successfully obtained TROs in eight other cases involving cybercriminals who were committing similar malicious acts–distributing malware, setting up botnets, and causing harm to Microsoft and its consumers.[1]

[1] *See* Haimovici Decl. Exs. 29-30, *Microsoft Corp. v. John Does 1-8*, No. 1:13-cv-01014 (W.D. Tex. Nov. 25, 2013, Dec. 12, 2013) (order granting *ex parte* TRO to dismantle botnet command-and-control servers and voluntary dismissal following success under TRO and plaintiff's desire to assist law enforcement); Ex. 31-32, *Microsoft v. John Does 1-82*, No. 3:13-cv-319 (W.D.N..C. May 29,

I. Microsoft Is Likely To Succeed On The Merits On Each Of Its Claims

The Complaint sets forth 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 Anti-Cybersquatting Consumer Protection Act (15 U.S.C. § 1125), (3) violations of Unlawful Acts Regarding Computers and Information Services Statute (N.R.S. § 205.473), (4) trespass to chattels/computer trespass, (5) conversion, and (6) negligence.

A. The Computer Fraud and Abuse Act

Microsoft asserts that Malware Defendants violated the Computer Fraud and Abuse Act. The Computer Fraud and Abuse Act ("CFAA") penalizes a party that does the following acts:

- Intentionally accesses a computer without authorization or exceeds authorized access,[2] and thereby obtains information from any protected computer (18 U.S.C. § 1030(a)(2)(C));
- Knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period (18 U.S.C. § 1030(a)(4);
- 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));

2013, Jun. 10, 2013) (order granting *ex parte* TRO to take down Citadel botnet and preliminary injunction); Ex. 33-34, *Microsoft v. John Does 1-18*, No. 1:13-cv-139 (E.D. Va. Jan. 31, 2013, Feb. 13, 2013) (orders granting *ex parte* TRO and preliminary injunction against defendants responsible for Bamital botnet); Exs. 35-36, *Microsoft v. Yong et al.*, No. 1:12-cv-1004 (E.D. Va. Sept. 10, 2012, Sept. 28, 2012) (order granting *ex part*e TRO to redirect botnet communications through 3222.org and its sub-domains and voluntary dismissal after settlement with defendants); Exs. 37-38, *Microsoft Corp. v. John Does 1-39*, No. 1:12-cv-01335 (E.D.N.Y. Mar. 19, 2012, Mar. 29, 2012) (orders granting *ex parte* TRO and preliminary injunction to dismantle botnet command-and-control servers); Exs. 39-40, *Microsoft Corp. v. Piatti*, No. 1:11-cv-1017 (E.D. Va. Sept. 22, 2011, Oct. 12, 2011) (same); Exs. 41-42, *Microsoft Corp. v. John Does 1-11*, No. 2:11-cv-00222 (W.D. Wash. Mar. 9, 2011, April 6, 2011) (same); Exs. 43-44, *Microsoft Corp. v. John Does 1-27*, No. 1:10-cv-00156 (E.D. Va. Feb. 22, 2010, Mar. 10, 2010) (same); *see also* Exs. 45-46, *FTC v. Pricewert LLC*, No. 09-2407 (N.D. Cal. June 2, 2009, June 15, 2009) (orders granting *ex parte* TRO and preliminary injunction disconnecting service to botnet hosting company).

[2] The term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled to obtain or alter. 18 U.S.C. § 1030(e)(6).

- Intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage (18 U.S.C § 1030(a)(5)(B)); or

- Intentionally accesses a protected computer[3] without authorization, and as a result of such conduct, causes damage[4] and loss[5] (18 U.S.C. § 1030(a)(5)(C)).

Malware Defendants intentionally send malicious code to Microsoft's and its customers' protected computers and operating systems, without authorization, in order to infect those computers. The evidence submitted in support of this motion demonstrates that Microsoft and its customers are damaged by this intrusion. These Defendants deceive consumers into downloading and then installing the malware without Microsoft's or its consumers' authorization. (Tan Seng Decl. ¶¶ 9-10.) Once installed, the malware runs without the customers' or Microsoft's knowledge or consent and specifically targets the Windows operating system. After the person's computer is infected with the malware, it is then subject to the control of the hacker. (*Id.* ¶¶ 21-23.) The hacker can use the victim's computer and the malware for any number of malicious purposes, such as stealing personal information stored on the system, hijacking the computer's camera and recording videos without the user's knowledge or consent, theft of personal data such as passwords and financial credentials through key-logging, click-fraud, sending requests to download other malicious software on the computer, or otherwise using it to carry out fraud, computer intrusions, or other malicious and illegal conduct. (*Id.*)

This is precisely the type of activity that the CFAA is designed to prevent. *See, e.g., Facebook, Inc. v. Fisher*, 2009 WL 5095269, at *2-3 (N.D. Cal. Dec. 21, 2009) (granting a TRO under CFAA where defendants allegedly engaged in a phishing and spamming scheme that compromised the accounts of Facebook users); *Physicians Interactive v. Lathian Sys.*, 2003 U.S.

[3] 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).

[4] The term "damage" means any impairment to the integrity or availability of data, a program, a system, or information. 18 U.S.C. § 1030(e)(8).

[5] The term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service. 18 U.S.C. § 1030(e)(11).

Dist. LEXIS 22868, at *30-31 (E.D. Va. Dec. 5, 2003) (granting TRO and preliminary injunction under CFAA where defendant hacked into a computer and stole confidential information); *Global Policy Partners, LLC v. Yessin*, 686 F. Supp. 2d 631, 635-37 (E.D. Va. 2009) (accessing computer using credentials that did not belong to defendant actionable under the CFAA). Indeed, some courts have appropriately observed that the CFAA was targeted at "computer hackers (e.g., electronic trespassers)." *State Analysis, Inc. v. Am. Fin. Srvcs. Assoc.*, 621 F. Supp. 2d 309, 315 (E.D. Va. 2009) (citation omitted).

B. The Anti-Cybersquatting Consumer Protection Act

Defendants have violated the Anti-Cybersquatting Consumer Protection Act ("ACPA") by having registered, trafficked in, or used domain names containing the terms "Microsoft" or "Windows," which are protected marks owned by Microsoft. The ACPA provides civil remedies for trademark holders seeking relief against parties infringing upon their marks in connection with website domain names. *Super-Krete Int'l, Inc. v. Sadleir*, 712 F. Supp. 2d 1023, 1030 (C.D. Cal. 2010). A plaintiff establishes civil liability for such "cyberpiracy" by proving that (1) the defendant registered, trafficked in, or used a domain name; (2) the domain name is confusingly similar or dilutive to a protected mark owned by the plaintiff; and (3) the defendant acted "with bad faith intent to profit from that mark." *DSPT Intern., Inc. v. Nahum*, 624 F.3d 1213, 1218-19 (9th Cir. 2010); *see also* 15 U.S.C. § 1125(d)(1)(A).

All three of these elements exist here. Defendant Vitalwerks is the registered owner of the No-IP domains, and it authorizes the Malware Defendants to use sub-domains of its registered domains that contain Microsoft's protected marks. (Haimovici Decl. ¶ 6.) The Malware Defendants in turn use these domains to communicate with infected computers and to further their botnet activities and other illegal schemes. The names of the sub-domains are confusingly similar to Microsoft's famous MICROSOFT and WINDOWS marks because they incorporate the correctly-spelled MICROSOFT or WINDOWS mark. *See* Ex. C to Compl. (listing 64 infringing domains); *see also Perfumebay.com Inc. v. eBay, Inc.*, 506 F.3d 1165, 1174-76 (9th Cir. 2007) (finding likelihood of confusion in trademark infringement case based on similarity of the challenged domain name, "perfumebay.com" to plaintiff's protected mark and domain name "ebay.com").

As for the third prong, the statute lists nine permissive factors that may be considered in "determining whether a person has bad faith intent." 15 U.S.C. § 1125(d)(1)(B)(i); *Lahoti v. VeriCheck, Inc.*, 586 F.2d 1190, 1202 (9th Cir. 2009). None of the factors favors Defendants. Defendant Vitalwerks owns and leases the Malware Domains, which the Malware Defendants use, and many of the domains are nearly identical to the domain for Microsoft's bona fide website at microsoft.com and all of which contain or are nearly identical to Microsoft's famous marks. Moreover, the Malware Domains serve no legitimate purposes. "The registration of typosquatting domains shows [Defendants]' intent to illicitly profit from the [Plaintiff's] mark, as there is no value independent of the infringement, as evidenced by the lack of association with any bona fide goods or services." *Facebook, Inc. v. Banana Ads LLC*, 2013 WL 1873289, at *7 (N.D. Cal. Apr. 30, 2013).

The eighth factor describes the Malware Defendants' bad faith exactly: "the person's registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties." 15 U.S.C. § 1125(d)(1)(B)(i). Registering and using multiple infringing domain names, combined with a lack of bona fide services and lack of other defenses, is sufficient for bad faith. *Banana Ads*, 2013 WL 1873289, at *7; *Pinterest, Inc. v. Qian Jin*, 2013 WL 5460821, at *2 (N.D. Cal. Sept. 30, 2013).

C. Nevada's Computer Fraud Statute

The Unlawful Acts Regarding Computers and Information Services Statute ("UARC") prohibits a person from "knowingly, willfully and without authorization" modifying, damaging, destroying, disclosing, using, transferring, concealing, taking, retaining possession of, copying, obtaining or attempting to obtain access to, permitting access to or causing to be accessed, or entering "data, a program or any supporting documents which exist inside or outside a computer, system or network." N.R.S. § 205.4765(1). UARC also prohibits similar conduct in regards to "equipment or supplies that are used or intended to be used in a computer, system or network" or simply directing such activities at "a computer, system or network." N.R.S. § 205.4765(2)-(3). UARC also makes a person subject to criminal and civil liability for "knowingly, willfully and

without authorization" obtaining and disclosing, publishing, transferring, or using "a device used to access a computer, network or data," or introducing, causing to be introduced or attempting to introduce a "computer contaminant into a computer, system or network."[6] N.R.S. § 205.4765(4-(5); *see also* N.R.S. § 205.511 ("Any victim of a crime described in N.R.S. [§§] 205.473 to 205.513, inclusive, may bring a civil action to recover: (a) Damages for any response costs, loss or injury suffered as a result of the crime; (b) Punitive damages; and (c) Costs and reasonable attorney's fees incurred in bringing the civil action.").

Here, Defendants Mutairi and Benabdellah knowingly, willfully and without authorization published and transferred the Bladabindi/Jenxcus malware to the Doe Defendants, and the Does knowingly, willfully and without authorization used the malware to access victims' computers, including the Microsoft operating system and data on those computers in violation of sections 205.4765(4) and (5). Malware Defendants have also violated section 205.4765(1) and (3) by enlisting the victims' computers into a botnet, exercising control over those computers, interfering with Microsoft's operating system or antivirus programs running on those machines, obtaining or attempting to obtain private information from those computers such as user names and passwords, snapshots of the user's desktop, and videos taken from the computer's video camera. (Tan Seng Decl. ¶¶ 21-23.)

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. *U-Haul Co. of Nev., Inc. v. U.S.*, 2011 WL 3273873, at *3 (D. Nev. July 29, 2011); *Oracle USA, Inc. v. Rimini Street, Inc.*, 2010 WL 3257933, at *5 (D. Nev. Aug. 13, 2010) (*quoting* RESTATEMENT (SECOND) OF TORTS § 218 (1965)); *Cerros v. North Las Vegas Police Dept.*, 2008 WL 608641, at *4 (D. Nev. Feb. 29, 2008) (*quoting* RESTATEMENT (SECOND) OF TORTS § 218 (1965)). Similarly, "the tort of conversion "'is a distinct act of dominion wrongfully exerted over personal property in denial of, or inconsistent with, title or rights therein or in derogation,

[6] The statute defines a computer contaminant to include a "virus, worm or Trojan horse." N.R.S. § 205.4737(2)(a).

exclusion or defiance of such rights.'" *U-Haul Co. of Nev., Inc.*, 2011 WL 3273873, at *3 (*quoting Edwards v. Emperor's Garden Restaurant*, 130 P.3d 1280, 1287 (Nev. 2006)); *see also Kremen v. Cohen*, 337 F.3d 1024, 1035-36 (9th Cir. 2002) (court held that Internet domain name could serve as basis for registrant's conversion claim under California law); *Thyroff v. Nationwide Mut. Ins. Co.*, 864 N.E.2d 1272, 1272, 1275-76 (N.Y. 2007) (conversion applies to electronic computer records and data).

Malware Defendants have interfered with and taken as their own Plaintiff's resources, by installing software that interferes with Microsoft's licensed Windows operating system and customer computers. The unauthorized installation of malware that allows control over the computer causes injury to the value of the Windows operating system and the infected computer itself. Thus, this conduct is an illegal trespass and also constitutes conversion. *Kremen*, 337 F.3d at 1034 (recognizing that hacking into a computer system and injuring data supports a conversion claim); *Astroworks, Inc. v. Astroexhibit, Inc.*, 257 F. Supp. 2d 609, 618 (S.D.N.Y. 2003) (in deciding motion to dismiss, court held plaintiff could maintain claim for conversion of his website); *Physicians Interactive*, 2003 U.S. Dist. LEXIS 22868, at *30-31 (TRO and preliminary injunction granted 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."); *State v. Riley*, 846 P.2d 1365, 1371 (Wash. 1993) (affirming conviction for "computer trespass" under Washington law for defendants' "hacking activity"); *see also Bancroft & Masters, Inc. v. Augusta Nat'l Inc.*, 223 F.3d 1082, 1089 (9th Cir. 2000) (in a case involving a domain name, the question on appeal was personal jurisdiction, but a majority joined in the opinion on the assumption defendant "engaged in tortious conduct" because it intended to effect a conversion of plaintiff's domain name).

E. Negligence

The elements of a claim for negligence are "(1) the existence of a duty of care, (2) breach of that duty, (3) legal causation, and (4) damages." *U.S. v. Miners Contracting and Support, Inc.*, 2014 WL 293438, at *2 (D. Nev. Jan. 24, 2014) (*quoting Sanchez v. Wal-Mart Stores, Inc.*, 221 P.3d 1276, 1280 (Nev. 2009)). Microsoft asserts that Defendants Vitalwerks is negligent because it

breached one or more duties of care it owed to Microsoft and its consumers by failing to take preventative or remedial measures to remedy the abuse of its services. These duties arise from: 1) best practices in the industry, 2) assumption of a duty through the company's representations to the public, including its Terms of Service, and 3) contractual obligations with the registry operators and ICANN.

First, Defendant Vitalwerks owed a duty of care to utilize the best practices in the industry that when implemented, would curb Malware Defendants use of No-IP for illegal activities. These best practices include:

- Require free Dynamic DNS subscribers to provide a name, address, telephone number, and IP address to register for a free sub-domain;
- Make the subscribers' information including sub-domain names publicly available in a searchable database;
- Use of a web reputation service that would identify bad sub-domain activity; and
- Encrypting No-IP user names and passwords and storing them someone other than the subscriber's registry.

(Lyons Decl. ¶ 21.)

By failing to collect and make available identifying information about its sub-domain subscribers, Defendant Vitalwerks makes its services susceptible to abuse. (*Id.*) Defendant also makes it service attractive to abuse because it fails to engage in best practices to keep its subscribers' user names and passwords safe, making it easy for bad actors to hack legitimate subscribers' accounts. (*Id.*) Moreover, Defendant Vitalwerks has been on notice since at least the beginning of 2013 that its services were being abused, and yet it failed to sufficiently monitor and block malicious sub-domain traffic by using tools available to it like web reputation services.

Second, Defendant Vitalwerks assumed a duty to monitor, detect, prevent, and remedy abuse of its services with the representations it made to the public, on its website and in blog postings, that it would do so. (Haimovici Decl. ¶¶ 31-34.) Defendant's own Terms of Service prohibits its subscribers from abusing or fraudulently using the No-IP service, interfering or tampering with another subscriber's use of the service, causing or attempting to cause harm to another computer or

network, or using the service in any way that violates the law or Internet regulations. (*Id.*, Ex. 5.) Defendants must also be held to this same standard of conduct. By reassuring the Internet security community, its customers, and the general public, all the while continuing to make its services attractive to abusers, Defendant voluntarily assumed a duty to prevent or stop the Malware Defendants' conduct. *See Wright v. Schum*, 781 P.2d 1142, 1145-47 (Nev. 1989) (holding that defendant voluntarily assumed a duty to protect against attack from another person's dog); *see also Harry v. Smith*, 893 P.2d 372, 375 (Nev. 1995) (noting that under *Wright*, a defendant has a "duty to protect third parties from dog bites" if the defendant "takes affirmative steps to assume a duty"); *Nev. Nat. Bank v. Gold Star Meat Co., Inc.*, 514 P.2d 651, 653-54 (Nev. 1973) (finding that bank employee under no duty to divulge credit disclosure information was required to exercise due care once he voluntarily disclosed such information). Again, Defendant breached these duties causing Microsoft and its consumers harm.

Last, Defendant Vitalwerks owed a duty of care to Microsoft and its customers that arose from its contractual relationships with the registry operators and ICANN. A contract can impose a duty of care, a breach of which could give rise to a claim for negligence. *Sharp Plumbing, Inc.* v. *Nat'l Fire & Marine Ins. Co.*, 2013 WL 6858895, at *9 (D. Nev. Dec. 27, 2013) (*quoting Calloway v. City of Reno*, 993 P.2d 1259, 1263 (Nev. 2000) ("In Nevada, '[a] breach of contract may be said to be a material failure of performance of a duty arising under or imposed by agreement.'")). To become an accredited registrar, Defendant Vitalwerks entered into agreements with ICANN and the registry operators that impose obligations on Defendant as the registrar and the registered name holder of the No-IP domains. (Haimovici Decl. ¶¶ 13-20.) Defendant Vitalwerks has contractual duties that require it to investigate and stop computer abuse that is being perpetuated through its services. Vitalwerks is bound by the registry-registrar agreements which prohibit abuse and require that registrants not use domains in an illegal manner. (*Id.* ¶¶ 21-30.)

Moreover, Defendant Vitalwerks, as an accredited ICANN registrar, has a duty to conduct its Internet business in such a manner that promotes accountability and discourages criminal activities, and it has breached this duty in several ways. (Haimovici Decl. ¶¶ 13-20.) Contrary to these agreements, Defendant Vitalwerks' failure to exercise due care enables the illegal conduct at issue in

this case. It provides the necessary infrastructure to direct malware-infected personal computers to the particular sub-domain through which the Malware Defendants control the malware infected computer. (Lyons Decl. ¶ 20; Anselmi ¶¶ 9-18.) Despite being on notice that its services are being abused, Defendant has failed to take sufficient corrective action. Similarly, the Malware Defendants by distributing malware and infecting user computers breached its obligations under No-IP's Terms of Service. (*See* Haimovici Decl. ¶¶ 6-8.)

II. Irreparable Harm Will Result Unless A TRO And Preliminary Injunction Are Granted

Microsoft is the provider of the Windows operating system and a variety of other software and services. (Lyons Decl. ¶ 4.) Microsoft has invested substantial resources in developing high-quality products and services. (*Id.*) Due to the high quality and effectiveness of Microsoft's products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, has established a strong brand, has developed the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. (*Id.*) Microsoft has registered trademarks representing the quality of its products and services and its brand, including the Windows marks. (*Id.*)

Defendants' activities injure Microsoft and its reputation, brand, and goodwill because customers subject to the negative effects of the malware incorrectly believe that Microsoft or Windows is the source of their computer problems. (*Id.* ¶ 22.) Additionally, Microsoft devotes significant computing and human resources to combating Bladabindi and Jenxcus malware infections and helping customers determine whether or not their computers are infected, and if so, cleaning them. (*Id.* ¶ 23.) Customers' frustration with having to deal with malware infections on their computers diminishes their regard for Windows and Microsoft, and tarnishes Microsoft's reputation and goodwill. There is also a serious risk that customers may move from Microsoft's products and services because of such activities. And, there are significant challenges to having such customers return, given the cost they bear to switch to new products and perceived risks.

This type of brand-related injury and customer harm is most certainly irreparable and is precisely why the relief requested in this motion should be granted. *See Stuhlbarg Intern. Sales Co.,*

Inc. v. John D. Brush and Co., Inc., 240 F.3d 832, 841 (9th Cir. 2001) ("Evidence of threatened loss of prospective customers or goodwill certainly supports a finding of the possibility of irreparable harm." (*citing Tom Doherty Assocs., Inc. v. Saban Entm't, Inc.*, 60 F.2d 27, 37-38 (2d Cir. 1995) ("in trademark licensing case, deprivation of opportunity to expand business is irreparable harm")); *Multi-Channel TV Cable Co. v. Charlottesville Quality Cable Operating Co.*, 22 F.3d 546, 552 (4th Cir. 1994) ("when the failing to grant preliminary relief creates the possibility of permanent loss of customers to a competitor or the loss of goodwill, the irreparable injury prong is satisfied . . . .").

Once infected, a person's computer is under the Malware Defendant's control. The Defendants can use the victim's computer for any number of malicious purposes, such as stealing personal information stored on the system, sending bulk, unsolicited "spam" emails, delivering malicious software to infect other computers or otherwise using it to carryout fraud, computer intrusions or other malicious and illegal conduct. (Tan Seng Decl. ¶¶ 8, 21-22.) With the malware dashboard, Defendants are able to execute many commands on users' computers that can steal sensitive information and invade the users' privacy. (*Id.*) For example, they can steal users' banking credentials, such as online user names, passwords, and account numbers. When a user conducts transactions online, the Defendant can monitor the user's keystrokes and capture home addresses, work addresses, telephone numbers, credit card information, and social security numbers. The Malware Defendants can see in real time users' computer displays and can also remotely turn on the users' video cameras or microphones without their knowledge, which is violative of many states' privacy and wiretapping laws. The information Defendants collect can be sold or traded to other wrongdoers and can even be used for blackmail. Consumers suffer not only economic harm as a result of Malware Defendants' actions but non-economic losses as well, such as emotional distress, from identity theft and intrusions upon privacy.

Additionally, users computers' performance may suffer due to the repeated copying of files, data transfer and connections to the Internet that the malware causes the person's computer to undertake without permission. And because customers are often unaware of the infection, they unknowingly allow their computers to be misused indefinitely. This is particularly true for the malware at issue here given its ability to conceal and protect itself and because there are numerous

iterations of it supported by No-IP's sub-domains. (*See id.* ¶ 24.) In such circumstances, technical attempts to remedy the problem may be insufficient and the injury caused to customers will continue. (*Id.*) The injury caused by Bladabindi and Jenxcus malware and No-IP extends far beyond Microsoft to other consumers and providers, into Internet infrastructure and ultimately to the majority of computer users worldwide, placing each at increased risk.

Continued operation and spread of the Bladabindi/Jenxcus malware irreparably harms Microsoft, its customers, and the public. No monetary remedy could repair the harm to Microsoft or its customers if Bladabindi/Jenxcus botnets are permitted to continue operating and spreading. Federal courts in civil cases addressing the unabated spread and harm of malware and botnets have concluded that the "immediate and irreparable harm" to consumers from such activities warranted an *ex parte* TRO and preliminary injunction. *See* Haimovi Decl. at Exs. 29, 37, 41 and 43, *Microsoft Corp. v. John Does 1-8, Microsoft Corp. v. John Does 1-39* and *Microsoft Corp. v. Piatti*, *Microsoft Corp. v. John Does 1-11*, and *Microsoft v. John Does 1-27* (acknowledging the substantial irreparable harm botnets cause Microsoft, its customers and Internet users generally). Microsoft and the public face the same irreparable harm caused by Bladabindi/Jenxcus as was found in those cases. Thus, entry of an *ex parte* TRO disabling the malware activity carried out though No-IP and an Order to Show Cause why a preliminary injunction should not issue are warranted.

Further, if the requested relief is not granted, the Bladabindi/Jenxcus malware will continue to spread and continue to infect the computers of Microsoft's customers. This injury is irreparable because customers, for the most part, lack the technical knowledge, skills, and ability to remedy the infection, if they are even able to detect the infection. In the absence of the requested relief, Microsoft's customers would remain under constant threat of their computers being infected and suffering the harmful effects of unauthorized intrusion into and abuse of their computers. Long term injury of this type constitutes irreparable harm warranting the entry of the requested relief. *See Arminius Schleifmittel GmbH v. Design Indus., Inc.*, 2007 WL 534573, at *6 (M.D.N.C. Feb. 15, 2007) (finding irreparable harm because defendant's action "will have significant and continuous long-term effects").

III. The Balance Of Hardships Tips Sharply In Microsoft's Favor

Defendants will suffer no harm to any legitimate interest if an *ex parte* TRO and preliminary injunction are issued. Cutting communications to No-IP sub-domains confirmed to be enabling malware will prevent Malware Defendants from sending instructions or additional malware modules to infected personal computers during that time and will preserve the evidence of the malwares' operations and illegal activities. Defendant Vitalwerks will suffer no harm if a TRO and preliminary injunction are issued because Defendant derives no known income form the operation of its free Dynamic DNS service. If there is any legitimate activity carried out on the No-IP sub-domains, it will be allowed to proceed under the terms of the proposed order with no disruption. (Anselmi Decl. ¶¶ 19-28.) Thus, Defendants will suffer no harm through preservation of the *status quo* pending adjudication of the issues in dispute. *See Allegra Network LLC v. Reeder*, 2009 WL 3734288, at *3 (E.D. Va. Nov. 4, 2009) (preliminary injunction issued where there was no evidence that the defendants would suffer irreparable harm from not being able to carry out enjoined activities).

Similarly, there will be only negligible impact on the third-party domain registries that will need to implement part of the proposed order. This limited assistance is necessary to ensure effective implementation of the requested order and is authorized under the All-Writs Act, 28 U.S.C. § 1651.

Conversely, if a TRO and preliminary injunction do not issue, Bladabindi/Jenxcus will continue to inflict irreparable injury on Microsoft, its customers, and the public. As this malware spreads and new users are infected each day, this dramatically increases the ability for illegal conduct to occur, compounding the injury to Microsoft and the public.

IV. The Public Interest Will Be Served By The Issuance Of A TRO And Preliminary Injunction

In understanding the beneficial impact a TRO and preliminary injunction will have on the pubic, it is exceedingly important to recognize the degree to which the TRO and preliminary injunction protects the public interest beyond Microsoft and its own customers. Every consumer, company, governmental agency, or other entity with access to the Internet is at risk of being irreparably injured by Bladabindi/Jenxcus supported by the No-IP sub-domains. There is an

overwhelming public interest in preserving the status quo and halting the growth of this malware while Microsoft proceeds with its claims.

Another district court emphasized in a similar case "a strong public interest in granting preliminary injunctive relief" and noted that "[t]his Court has an obligation to enjoin any alleged computer hackers from continuing to attack and steal [plaintiff's] proprietary information." *Physicians Interactive*, 2003 U.S. Dist. LEXIS 22868, at *30-31 (granting TRO and preliminary injunction where defendant hacked into a computer and stole confidential information). In the botnet context, district courts in recent years have concluded that "immediate and irreparable harm" will result to the welfare of consumers form "botnet command-and-control servers" and the malicious conduct carried out though botnets. (*See*, *e.g.,* Haimovici Decl., Exs. 29, 31-35, 37-39, 41-46.) Similarly, here a TRO and preliminary injunction will preserve and protect this important public interest. No such protection will be afforded if preliminary relief is denied and, in that event, the Defendants controlling the malware and botnets will be able to continue their activities with impunity.

V. ***Ex Parte*** **Relief Is Necessary to Stop the Irreparable Harm to Microsoft And the Public**

Rule 65 of the Federal Rules of Civil Procedure permits an *ex parte* TRO where the moving party sets forth facts that show an immediate and irreparable injury and why notice should not be required. Fed. R. Civ. P. 65(b)(1); *see Granny Goose Foods, Inc. v. Teamsters*, 415 U.S. 423, 438-39 (1974) ("Ex parte temporary restraining orders are no doubt necessary in certain circumstances . . . ."); *Hoechst Diafoil Co. v. Nan Ya Plastics Corp.*, 174 F.3d 411, 422 (4th Cir. 1999) ("temporary restraining orders may be issued without full notice, even, under certain circumstances, *ex parte* . . . ."). In this District Court, Local Rule requires that the application or motion "contain a statement showing good cause why the matter was submitted to the Court without notice to all parties." L.R. 7.5(b). Without a TRO granting the relief requested, the injury to Microsoft and the public, including Microsoft's customers, will continue unabated, irreparably harming Microsoft's reputation, brand and goodwill. In order for the TRO to be effective at all, it must issue *ex parte*. Here, the extraordinary factual circumstances warrant such relief.

A. If Notice is Given, the Malware Defendants Will Disappear and Change Their Online Identities, Rendering Microsoft's Efforts to Stop Their Conduct Fruitless

Good cause exists to justify this *ex parte* application and the relief requested. Microsoft seeks this TRO to put a stop to the harm caused by the Bladabindi/Jenxcus malware and requests an order that will allow it to block traffic between infected computers and malicious sub-domains controlled by No-IP, through which the Malware Defendants communicate with the infected computers. Microsoft has been unable through diligent investigation to pinpoint the exact locations of the Malware Defendants and for other bad actors responsible for the harm alleged in the Complaint, Microsoft is unaware of their true identities. However, these Defendants have a significant online presence and conduct their illegal activities by virtual means. Given the transient nature of the Internet and cybercriminals' ability to thwart detection, advanced notice to these Defendants of the TRO would provide them an opportunity to essentially vanish into thin air and restart their criminal activities under different online aliases, using differing computers, servers, and other infrastructure. (Lyons Decl. ¶ 24.)

Defendants are also likely to take steps to destroy information relating the malware distribution and botnet scheme. Infected computers may be reprogrammed to contact command-and-control computers at different IP addresses and through different sub-domains, enabling Malware Defendants to continue controlling the infected computers without disruption. (*Id.*) If the command-and-control computers are moved, Microsoft's investigation into Defendants' illegal activities would have to be restarted. Thus, notice before issuance of the TRO relief would permit the Malware Defendant to continue their harmful activity and would render Microsoft's efforts to investigate and combat this type of abuse moot.

It is well-established that *ex parte* relief is appropriate under circumstances such as the instant case, where notice would render the requested relief "fruitless." *See, e.g., In the Matter of Vuitton Et Fils S.A.*, 606 F.2d 1, 4 (2d Cir. 1979) (*per curiam*) (holding that notice prior to issuing TRO was not necessary where notice would "serve only to render fruitless further prosecution of the action"; prior experience taught that once one member of the counterfeiting enterprise received notice, contraband would be transferred to another unknown counterfeiter, perpetuating the harm and

rendering judicial efforts pointless); *AllscriptsMisys, LLC v. Am. Digital Networks, LLC*, 2010 U.S. Dist. LEXIS 4450, at *2 (D. Md. Jan. 20, 2010) (granting an *ex parte* TRO where "Defendant may dissipate the funds and/or take action to render it difficult to recover funds . . . .").[7]

Here, the danger imposed by advanced notice is real and not vague or speculative. There is specific evidence that botnet operators have attempted to evade prior enforcement attempts where they had notice, by moving for example their command-and-control servers. Particularly instructive here is *Microsoft Corp. v. John Does 1-27*, where, in February 2010, the Eastern District of Virginia issued an *ex parte* TRO and supplemental *ex parte* TRO suspending 276 Internet domains used to control a malicious botnet. (*See* Haimovici Decl., Ex. 43, *Microsoft Corp.*, No. 1:10-cv-156 (E.D. Va. Feb. 22, 2010) (order granting TRO)). In issuing the *ex parte* TRO, the court acknowledged that:

> There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result form the sale, transfer, or other disposition or concealment by Defendants of the domains at issue in Microsoft's TRO Motion and other discovery evidence of Defendants' misconduct available through such domains if the Defendants receive advance notice of this action . . .

(*Id*. at ¶ 4.)

Additionally, in *FTC v. Pricewert LLC*, the Northern District of California issued an *ex parte* TRO suspending Internet connectivity of a company enabling botnet activity and other illegal computer-related conduct on the basis that "Defendant is likely to relocate the harmful and malicious code it hosts and/or warn its criminal clientele of this action if informed of the [plaintiff's] action." (*See* Haimovici Decl. Ex. 45, *FTC v. Pricewert LLC*, Case No. 09-2407, at 3 (N.D. Cal. 2009) (Whyte, J.)). Moreover, the court in *Dell, Inc. v. BelgiumDomains, LLC*, 2007 WL 6862341, *1-2 (S.D. Fla. Nov. 21, 2007), issued an *ex parte* TRO against domain registrants where persons similarly situated had previously concealed such conduct and disregarded court orders by using fictitious business, personal names, and shell entities to hide their activities. *Id.* at *2. In *Dell*, the

[7] *Crosby v. Petromed, Inc.*, 2009 WL 2432322, at *2 (E.D. Wash. Aug. 6, 2009) (granting *ex parte* TRO as "notice to Defendants of this TRO request could result in further injury or damage to Plaintiffs . . . .").

court explicitly found that where, as here, defendants' scheme is "in electronic form and subject to quick, easy, untraceable destruction by Defendants," *ex parte* relief is particularly warranted. *Id.* at *2.

B. If Notice is Given, Evidence Regarding the Malware Will be Destoryed, Disturbing the Status Quo

If notice is given in advance of a TRO, evidence of the Bladabindi/Jenxcus malware distribution may be destroyed. In particular, upon notice, account information pertaining to Malware Defendants operating the No-IP sub-domains associated with the malware may be destroyed. (*See* Lyons Decl. ¶ 24.) Further, if the malware operators attempt to reprogram the infected personal computers to communicate with domains which are not No-IP sub-domains, additional evidence will be lost, such as the identity of infected user computers and other aspects of the system necessary to this litigation. (*Id.*) Under such circumstances, courts have issued *ex parte* TROs. *See AT&T Broadband v. Tech Commc'ns, Inc.*, 381 F.3d 1309, 1319-1320 (11th Cir. 2004) (affirming *ex parte* search and seizure order to seize contraband technical equipment, given evidence that in the past defendants and persons similarly situated had secreted evidence once notice given); *Dell, Inc.*, 2007 WL 6862341, at *1-2; *Little Tor Auto Center v. Exxon Co., U.S.A.*, 822 F. Supp. 141, 143 (S.D.N.Y. 1993) (*ex parte* TRO appropriate where contraband "may be destroyed as soon as notice is given"). For this reason, the requested *ex parte* TRO is warranted.

VI. Microsoft Will Make Extraordinary Efforts To Provide Notice Of The TRO And The Preliminary Injunction Hearing And To Serve The Complaint

To ensure Due Process, immediately upon entry of the requested *ex parte* TRO, Microsoft will undertake extraordinary efforts to effect formal and informal notice of the preliminary injunction hearing to the Defendants and to serve the complaint as follows.

C. Microsoft Will Provide Notice to Defendant Vitalwerks by Personal Service

Defendant Vitalwerks is a limited liability company that operates from a physical address in Reno, Nevada. (Haimovici Decl. ¶ 2.) Pursuant to Rule 4(h)(1)(A), a defendant corporation, partnership, or other unincorporated association must be served "in the manner prescribed by Rule 4(e)(1) for serving an individual." Under Rule 4(e)(1), service is effected under the laws of the state

in which the district court is situated or where service is made. Nevada law permits service on any member of a "member-managed limited liability company." Nev. R. Civ. Pro. 4(d)(1)(iv).

Defendant Vitalwerks is a member-managed limited liability company, and Daniel Durrer is a managing member of the company and also its registered agent. (Haimovici Decl. ¶ 2.) Microsoft plans to effect formal service of the notice of the preliminary injunction hearing by personal delivery of the summons, complaint, and instant motion and supporting documents, and any order issued by this Court to Daniel Durrer at Defendant Vitalwerks' Reno address. (*Id.* ¶ 35.)

D. Microsoft Will Provide Notice to Defendants Mutairi and Benabdellah by E-mail, Skype, Facebook, and Publication

After conducting a thorough and diligent investigation, Microsoft has been unable to locate postal addresses for Defendants Mutairi and Benabdellah.[8] (Haimovici Decl. ¶ 36.) Microsoft has identified e-mail addresses, Skype, and Facebook accounts for these Defendants. (*Id.*, *see also* Tan Seng Decl. ¶¶ 30-33.) Microsoft will provide notice of the preliminary injunction hearing by immediately sending the same pleadings described above to Defendants by email, Skype, and Facebook, and Microsoft will publish the notice and pleadings on a centrally located, publically accessible source on the Internet for a period of 6 months. (Haimovici Decl. ¶¶ 39-41.)

Legal notice and service by e-mail, social media websites, and publication satisfies Due Process as these means are reasonably calculated, in light of the circumstances, to apprise the interested parties of the TRO, the preliminary injunction hearing, and the lawsuit. *See Mullane v. Central Hanover Bank & Trust Co.*, 339 U.S. 306, 314 (1950). Methods other than mail notice and service are \authorized under Federal Rule of Civil Procedure 4(f)(3), which allows a party to serve defendants by means not prohibited by international agreement. The methods of notice and service proposed by Microsoft have been approved in other cases involving international defendants attempting to evade authorities. *See*, *e.g.*, *Rio Properties, Inc. v. Rio Int'l Interlink*, 284 F.3d 1007, 1014-15 (9th Cir. 2002) (authorizing service by e-mail upon an international defendant); Haimovici Decl., Ex. 47, *FTC v. PCCare247, Inc.*, No. 1:12-Civ-7189, at 8-9 (S.D.N.Y. Mar. 7, 2013) at 8-9

[8] Because Microsoft does not have postal addresses for these Defendants, the Hague Convention on service or process does not apply. (Haimovici Decl. ¶ 38.)

(order permitting service by Facebook as supplemental means to e-mail service); Haimovici Decl., Ex. 35, *Microsoft Corp. v. Yong et al.*, No. 1:12-cv-1004, at 6-7 (E.D. Va. Sept. 10, 2012) (*ex parte* order giving Microsoft authority to serve foreign defendants by e-mail and publication); *Banana Ads*, 2012 WL 1038752, at *2 (granting Facebook's motion to serve foreign cybersquatter defendants by e-mail); *AllscriptsMisys, LLC*, 2010 U.S. Dist. LEXIS 4450, at *3 (granting *ex parte* TRO and order prompting notice by telephone, e-mail, mail, or other delivery services); *Smith v. Islamic Emirate of Afghanistan*, 2001 WL 16582111, at *2-3 (S.D.N.Y. Dec. 26, 2001) (authorizing service by publication upon Osama bin Laden and the al-Queda organization).

The party seeking to serve a foreign defendant by alternative means pursuant to Rule 4(f)(3) must demonstrate that (1) the service is "'reasonably calculated to provide actual notice' to the defendant," and (2) "international agreement does not prohibit such service." *Banana Ads*, 2012 WL 1038752, at * 1 (citing to *Rio Properties*, 284 F.3d at 1016). Here, both conditions are met.

1) Service by e-mail, Skype, Facebook, and publication on the Internet is reasonably calculated to provide Defendants with actual notice

First, Microsoft's proposed methods of service are reasonably calculated to provide actual notice to Defendants Mutairi and Benabdellah given the circumstances of this case. Defendants Mutairi and Benabdellah have established online identities through which they publish and distribute malware. (Tan Seng Decl. ¶¶ 31-33.) These Defendants maintain active Twitter, Skype, and Facebook accounts, and Defendant Mutairi also maintains several blogs and a website and posts content to YouTube about the Bladabindi malware. (*Id.*; *see also id.* ¶ 25.) These Defendants rely on the Internet and electronic means of communication to further their criminal and malicious scheme, and e-mail, Facebook, and publication are the only methods by which Microsoft has to notify the Defendants, whose addresses are unknown, of the present lawsuit and any preliminary injunction hearing.

In cases such as this one where defendants regularly conduct business or other transactions through electronic means and service on a physical address is not possible, service by e-mail and publication is reasonably calculated to provide actual notice. *See Banana Ads*, 2012 WL 1038752, at *2; *Aevoe Corp. v. Pace*, 2011 WL 3904133, at *2 (N.D. Cal. Sept. 6, 2011) (service by e-mail and

publication appropriate when plaintiff could not serve cybersquatting defendants by personal or mail service at several known addresses or by hiring a private investigator). And, as the Ninth Circuit has observed, e-mail service is particularly warranted in cases involving Internet-based misconduct, carried out by international defendants, causing immediate and irreparable harm:

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

Rio Properties, 284 F.3d at 1018; *see also Williams-Sonoma, Inc. v. Friendfinder, Inc.*, 2007 WL 1140639, at *2 (N.D. Cal. Apr. 17, 2007) (service by e-mail consistent with Hague Convention and warranted in case involving misuse of Internet technology by international defendants).

In this case, the e-mail addresses used by Defendant Mutairi and Benabdellah to conduct their malicious activities are the most accurate and viable contact information and means of notice and service. Moreover, Microsoft will supplement this form of service by also providing notice through Facebook and by publication. Microsoft has located e-mail addresses and Facebook accounts for these Defendants, and this contact information has been verified as belonging to the individuals who created and distribute the malware at issue in this lawsuit. Service by Skype and Facebook message and publication is warranted here as extra means to ensure actual notice to Defendants. *See FTC v. PCCare247, Inc.*, No. 1:12-Civ-7189, at 8-9 (S.D.N.Y. Mar. 7, 2013) (order finding that service by Facebook satisfies Due Process when used as a supplemental form of notice and plaintiff set forth sufficient facts demonstrating that the Facebook accounts belong to defendants), attached as Ex. 47 to Haimovici Decl.; *BP Products North America, Inc. v. Dagra*, 236 F.R.D. 270, 272-73 (E.D. Va. 2006) (discussing that publication on foreign defendant comports with Due Process when traditional means of service are unavailable and publication is likely to reach defendant).

2) Service by e-mail, Skype, Facebook, and publication on the Internet is not prohibited by international agreement

Here, there is no international agreement between the United States and Defendants' countries of residence that prohibits service by e-mail, Skype, Facebook, and publication. To start, the United States and Kuwait are parties to the Hague Convention on Service Abroad of Judicial and Extrajudicial Documents. (Haimovici Decl. ¶ 37.) However, nothing in the Hague Convention expressly prohibits service by the alternative methods Microsoft is proposing pursuant to Rule 4(f)(3). *Banana Ads*, 2012 WL 1038752, at *2 (e-mail service not prohibited by Hague Convention); *FTC v. PCCare247, Inc.*, No. 1:12-Civ-7189, at 8-9 (S.D.N.Y. Mar. 7, 2013) at 8-9 (Facebook service not prohibited by Hague Convention), Ex. 47 to Haimovici Decl.; *S.E.C. v. Anticevic*, 2009 WL 361739, at *4 (S.D.N.Y. Feb. 13, 2009) (service by publication not prohibited where countries did not expressly object to this type of service in their declarations pursuant to the Hague Convention). Additionally, Kuwait did not object to these forms of service in their declarations to the Convention. (*See* Haimovici Decl., Ex. 28.)

Similarly, there is no agreement between the United States and Algeria that prohibits service by e-mail, Skype, Facebook, or publication. If the defendant's resident country does not have an agreement in place expressly disavowing a particular type of service, then that service is permissible under Rule 4(f)(3). *See Rio Properties*, 284 F.3d at 1014 (noting that alternative service is proper if not prohibited by international agreement even if such service is "in contravention of the laws of the foreign country"); *JBR, Inc. v. Cafe Don Paco, Inc.*, 2013 WL 1891386, at *5 (N.D. Cal. May 6, 2013) (finding that e-mail service against defendant was permissible because Nicaragua was not a signatory to any agreement prohibiting this type of service); *see also* Jul. 26, 2010 Order in *Craigslist, Inc. v. Meyer et al.*, Case No. C 09-4739 SI (N.D. Cal.) (finding no agreements between U.S. and Thailand that would prohibit e-mail service), attached as Ex. 48 to Haimovici Decl.; *Bank Julius Baer & Co. Ltd. v. Wikileaks*, 2008 WL 413737, at *1-2 (N.D. Cal. Feb. 13, 2008) (finding that service through e-mail was not prohibited by international agreement); *Williams-Sonoma Inc.*, 2007 WL 1140639, at *2.

E. Microsoft Will Provide Notice To Doe Defendants By Publication.

Microsoft is unaware of the identities of Doe Defendants 1 through 500. However, Microsoft will provide notice of the preliminary injunction hearing and a copy of the summons, complaint, TRO motion and supporting documents to these Defendants by publication and any other method ordered by this Court.

CONCLUSION

For the reasons stated above, Microsoft respectfully requests that this Honorable Court grant its motion for a TRO and order to show cause regarding a preliminary injunction. Microsoft further respectfully requests that the Court permit notice of the preliminary injunction hearing and service of the Complaint by alternative means.

Dated: June 19, 2014

Respectfully submitted,

SHOOK, HARDY & BACON, L.L.P.

/s/ Tony M. Diab

TONY M. DIAB
Attorneys of Record for
Plaintiff Microsoft Corporation