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

MICROSOFT CORPORATION, a Washington corporation, Plaintiff, v. DOMINIQUE ALEXANDER PIATTI, an individual, DOTFREE GROUP S.R.O., a Czech limited liability company and JOHN DOES 1-22, CONTROLLING A COMPUTER BOTNET THEREBY INJURING MICROSOFT AND ITS CUSTOMERS Defendants.	Civil Action No: 1:11CV1017 **FILED UNDER SEAL**

BRIEF IN SUPPORT OF APPLICATION OF MICROSOFT CORPORATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

Plaintiff Microsoft Corp. ("Microsoft") seeks an emergency *ex parte* temporary restraining order ("TRO") and preliminary injunction to halt the growth of the Kelihos botnet ("Kelihos") that causes extreme and continued irreparable harm to Microsoft, its customers, and the public.

Botnets are computer networks consisting of tens of thousands, and can grow to millions, of compromised end-user computers. These end-user computers are infected with malicious software ("malware"), transforming them into tools for criminal activity that varies from disseminating enormous volumes of spam email, to attacking other computers on the Internet, to stealing financial and other personal information. Botnets, simply put, are plagues on the Internet, afflicting end users, corporations, and governments alike.

The Kelihos botnet is no different, causing extreme and irreparable injury to Microsoft, its customers, and the public. Kelihos illegally infects Internet users' computers with malicious software ("malware") that allows the botnet controllers to illegally manipulate the Kelihos-infected end-user computers and use them for a variety of illicit activities, including the capability of sending out billions of spam email messages, harvesting users' personal information (such as emails and passwords) and advertising dangerous counterfeit pharmaceuticals, fraudulent stock scams, and in some instances, websites for child pornography. By targeting Microsoft's Hotmail accounts and Windows operating system, Kelihos injures Microsoft's reputation, brand and goodwill, as Microsoft's customers are led to incorrectly believe that Microsoft, the provider of Hotmail and Windows, is the cause of the harmful spam. Kelihos, moreover, by using the infected computers to carry out illicit activities, has severe and negative impacts on the compromised user computers by reducing their performance.

Unchecked, Kelihos will continue to irreparably harm Microsoft, its customers, and the general public. Kelihos consists of 41,000 compromised end-user computers and continues to grow. The requested TRO directs the disabling of Kelihos' Command and Control Servers, specialized computers and software residing at Internet Protocol (IP) addresses and Internet ".com" and ".cc" domains that provide instructions to infected end-user computers.

Defendants Dominique Alexander Piatti, dotFree Group s.r.o. and John Doe Defendants 1-22 (collectively "Defendants") are the registrants of the two IP addresses and the twenty one Internet domains – identified in Appendices A and B to the Complaint. The purpose of those IP addresses and domains is to instruct the Kelihos infected-computers to engage in illegal activity, including the dissemination of spam email, to infect other end-user computers in order to expand the botnet, steal individual's personal information, or engage in some other form of cybercrime. Disabling the IP addresses and domains at issue here will stop the Kelihos botnet by severing communication between the botnet controllers and the infected end-user computers. Critically, once disabled, the IP addresses and Internet domains acting as Command and Control Servers will be unable to instruct the infected end-users computers, rendering Kelihos impotent.

Ex parte relief is essential here. Notice to Defendants would provide them an opportunity to destroy, move, conceal, or otherwise make inaccessible the instrumentalities used to direct Kelihos and the primary evidence of their unlawful activity. Giving them that opportunity would render further prosecution of this lawsuit entirely fruitless. Equally important, the IP addresses and domains must be disabled simultaneously to prevent any one Defendant from redirecting portions of the infected-computers to backup Command and Control servers, allowing the harm to continue.

This *ex parte* relief is not uncommon when disabling dangerous botnets. In a February 2010 case concerning the "Waledac" botnet, the District Court for the Eastern District of Virginia (Judge Brinkema presiding) addressed the risk inherent with a TRO by adopting an approach where:

1. the Court issued a tailored *ex parte* TRO, including provisions sufficient to effectively disable the harmful botnet infrastructure and stop irreparable harm being inflicted on Microsoft, its customers, and the public;
2. Microsoft, immediately after implementing the TRO, undertook a comprehensive effort to provide notice of the preliminary injunction hearing and to effect service of process on the defendants, including Court-authorized alternative service by email, mail, facsimile, publication and treaty-based means; and
3. after Microsoft provided notice, the Court held a preliminary injunction hearing, and granted the preliminary injunction while the case proceeded to ensure that harm caused by the botnet could not continue during the action.

See Microsoft v. John Does 1-27, Case No. 1:10-cv-00156 (E.D. Va. 2010, Brinkema, J.) (orders attached to the Declaration of Gabriel M. Ramsey ("Ramsey Decl."), Exs. 16, 17). More recently in March 2011, the District Court for the Western District of Washington adopted a similar approach in a case concerning the "Rustock" botnet, granting Microsoft *ex parte* relief to disable the botnet and issuing a preliminary injunction after Microsoft's comprehensive efforts to provide notice of the preliminary injunction hearing and effect service on the defendants. *See*

Microsoft v. John Does 1-11, Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.) (attached as Exs. 18, 19 to Ramsey Decl.).

Those approaches are appropriate here. If the Court grants Microsoft's requested relief, Microsoft will immediately make a robust effort in accordance with the requirements of Due Process to provide notice of the preliminary injunction hearing and to effect service of process on Defendants. Microsoft will immediately serve the complaint and all papers in this action on Defendants, using contact information maintained by the third-party hosting companies and domain registrars that host Defendants' command and control infrastructure.

I. STATEMENT OF FACTS: KELIHOS' ARCHITECTURE PROVIDES A SOPHISTICATED PLATFORM FOR ILLEGAL ACTIVITY

A "botnet" is a collection of individual computers, each running software that allows communication among those computers and includes computers providing control instructions to the rest of the botnet computers. (Declaration of Mark Debenham ("Debenham Decl."), ¶¶ 3-9, 20-41; Declaration of Jesse Kornblum ("Kornblum Decl."), ¶¶ 3-14). Malicious and criminal actors 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.*) Botnets provide a very efficient means of controlling huge numbers of computers and targeting any action internally against the contents of those computers or externally against any computer on the Internet. (*Id.*)

A. Overview of the Kelihos Botnet

The Kelihos botnet is made up of computers belonging to individual users who have unknowingly downloaded malicious software that infects their computers and renders them part of the botnet. (Debenham Decl., ¶¶ 4-7, 14-19, Exs. 2-3) A user may, for example, inadvertently interact with a website, email attachment, or download a fraudulent software product that contains the malicious botnet source code. (*Id.*) The malicious code infects the user's computer, making it part of the botnet. (*Id.*) The spread of the Kelihos botnet in this way

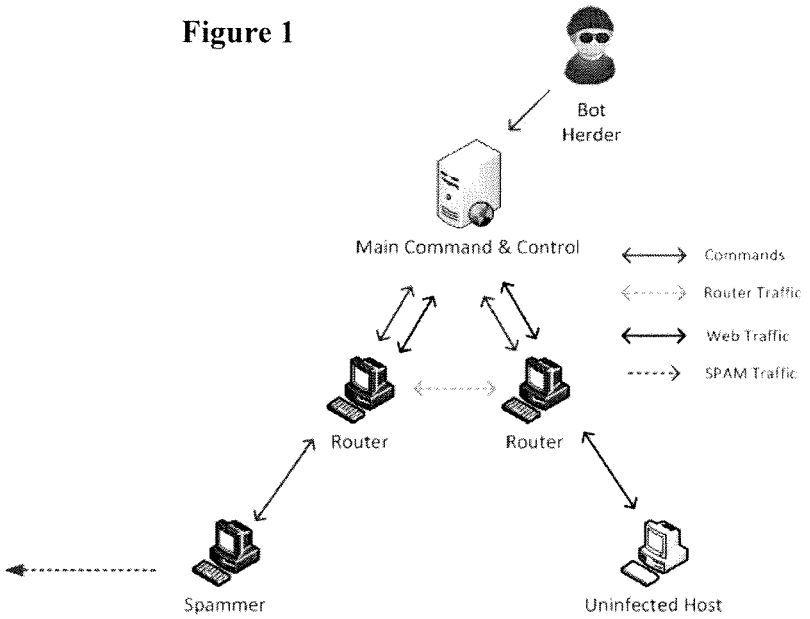
is not related to any vulnerability in Microsoft's systems, but is instead achieved by misleading unwitting users into taking steps that result in the infection of their machines. (*Id.*)

Once part of the botnet, the botnet controllers can now control the user's computer. (Debenham Decl. ¶¶ 20-32.) The parties controlling the botnet steal personal information – such as email addresses – from the user's computer. (*Id.* ¶ 41.) They can even cause a user's computer to send billions of bulk, unsolicited, harmful "spam" emails every day, deliver malicious software to infect other computers or otherwise use it to carry out fraud, computer intrusions or other malicious and illegal conduct. (*Id.* ¶¶ 6, 33-40, Exs. 9-10.)

The Kelihos botnet is created and controlled by a sophisticated organization that perpetrates unlawful conduct and has the capability of sending *3.8 billion spam emails* per day. (Debenham Decl. ¶ 33.) It is believed that the botnet is used to conduct activities that directly generate profits, such as sending unsolicited, harmful spam email in order to improperly generate advertising revenue. The parties in control of the botnet also sell capacity on the botnet to others who carry out such activities. (*Id.* ¶ 36.)

Microsoft has carefully studied the Kelihos botnet's architecture, design, and functions. (Debenham Decl. ¶ 3.) The Kelihos botnet consists of a tiered architecture. The lowest tiers of computers in the architecture consist of nearly 41,000 Kelihos-infected end-user computers. (*Id.* ¶¶ 5-9.) These tiers perform Kelihos' daily illegal activities, such as sending out enormous volumes of spam email. (*Id.*) Some such infected computers are merely used to relay and "proxy" communications between computers in the botnet and the outside world, to obfuscate the source of communications. (*Id.*) At the highest level in Kelihos' architecture – the "Command & Control Tier" – consists of specialized Command and Control servers that relay commands and information to the Kelihos-infected end-user computers. (*Id.*) The botnet controllers use the Command and Control Servers to deliver instructions to the Kelihos-infected end-user computers to carry out various illegal activities. (*Id.*) This hierarchical architecture is depicted in Figure 1 as follows:

Figure 1



1. The Kelihos Botnet Consists Of Nearly 41,000 End-User Computers

The Kelihos architecture consists of a large number of Kelihos-infected end-user computers commonly found in businesses, living rooms, schools, libraries, and Internet cafes around the world. (Debenham Decl. ¶ 25.) Microsoft detected nearly 41,000 instances of computers infected with some version of Kelihos botnet software. (*Id.*) A number of these computers connected to the Internet from IP addresses located in the Eastern District of Virginia. (*Id.* ¶ 19)

Analysis by Microsoft and independent researchers indicate that Kelihos uses deceptive methods to infect end-user computers. One method involves victims receiving an "e-card" by email, which appears to come from someone the victim knows, and which contains a link to a domain. When the victim clicks on the domain, their computer becomes infected and part of the Kelihos botnet. (Debenham Decl. ¶ 15, Exs. 2-3.) Defendants are generally engaged constantly in infecting additional end-user computers with Kelihos malware. Numerous software providers and software security firms are constantly engaged in trying to disinfect those computers. (*Id.* ¶¶ 20-24) That, however, is a complex task: owners of infected computers would need to undertake a specific investigation to even become aware of the infection, something many consumers are unable to undertake independently. (*Id.*)

Once infected, Defendants direct theses Kelihos-infected end-user computers to generate and send out a staggering volume of unsolicited email, commonly known as "spam." (Debenham Decl. ¶¶ 33-40, Exs. 7, 9-10.) While day to day volumes vary, it is estimated that the Kelihos botnet has the capability of disseminating approximately 3.8 billion spam emails per day. (*Id.*) Much of the Kelihos-generate spam promotes:

- stock scams that contains content attempting to entice users to purchase cheap stock in volume, artificially increasing the stock's price;
- pharmaceutical spam containing offers for purported male-enhancement pharmaceuticals that are often not legitimate branded products but rather are counterfeit or of questionable value or efficacy;
- advertisements for adult websites; and
- spam emails containing apparent promotions for child pornography.
- counterfeit goods, such as counterfeit watches
- "work from home" scams
- computer viruses

(*Id.* ¶¶ 38-39, Ex. 9-10.)

Most if not all owners of Kelihos-infected computers are unaware that their machines are infected and operating as part of the Kelihos botnet, or that their computers are sending out spam messages. (Debenham Decl. ¶¶ 20-24.)

2. Defendants Command The Kelihos-Infected End-User Computers Through Command And Control Servers

Critical to Kelihos are its Command and Control Servers that consist of Internet Protocol (IP) addresses and ".com" and ".cc" domains that Defendants have leased or purchased. (Debenham Decl. ¶¶ 10-18, Exs. 1-3, 8.) Command and Control Servers refers either physical server computers or software running on computers that support the Kelihos botnet.

Defendants here use the Command and Control Servers to continuously control the Kelihos-infected end-user computers. (Debenham Decl. ¶¶ 10-18.) Presently, 2 IP addresses

and 21 domains operate on the Internet as Kelihos Command and Control Servers. (*Id.*) Disabling these IP addresses and domains will disable the Kelihos Botnet. (*Id.* ¶¶ 42-45.) The number and locations of the Command and Control Servers may change over time, thus the requested relief is time sensitive as it must be implemented before the control servers again change.

The 2 IP addresses and 21 domains continuously control the ability of the Kelihos-infected end-user computers to communicate with each other and to expand the botnet. (Debenham Decl. ¶¶ 12-18.) The Kelihos Command and Control Servers send Kelihos-infected end-user computers information and instructions over the Internet that force the Kelihos-infected end-user computers to send out spam messages without the knowledge, approval, or involvement of the end-users. (*Id.* ¶¶ 21, 33-40.)

If a Kelihos-infected computer is unable to continue perpetuating the growth of the botnet, to send out malicious command to other computers, or to disseminate spam emails from the botnet, the Kelihos-infected computer will automatically communicate back to the Command and Control servers designated at these IP addresses for instructions about how to continue carry out the illicit activities. (Debenham Decl. ¶¶ 13-14.) As a failsafe, a Kelihos-infected botnet end-user computer that is unable to communicate with the 2 IP address will look to any of the 21 domains for instructions on how to continue to carry out these activities. (*Id.*) Links to these 21 domains, moreover, may be included in unsolicited spam email sent out by the botnet with the purpose of spreading the botnet to yet uninfected end-user computers. (*Id.* ¶ 15) These emails usually mislead the recipient by appearing to link to an e-card. (*Id.*) When the victim opens the link in the email, the botnet may deliver software that infects the victim's computer and makes it part of the Kelihos botnet. (*Id.*)

The purpose of the 2 IP address and 21 Internet domains that make up the Kelihos Command and Control servers is to await requests from Kelihos-infected computers and instruct them on how to control communication with each other and to infect new user

computers. (Debenham Decl. ¶ 18.) In this way, the domains and IP addresses support, propagate, and grow the botnet and enable the malicious activities Kelihos carries out.

B. Kelihos Directly Injures Microsoft's Customers

1. Overview Of Harm To Microsoft's Customers

Microsoft is a provider of the Windows operating system, Hotmail e-mail services and a variety of other software and services. (Debenham Decl., ¶ 20.) 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 and Hotmail marks. (*Id.*)

Kelihos' activities and the numerous resulting injuries to the public at large and Microsoft's customers, injure Microsoft and its reputation, brand and goodwill because users subject to the negative effects of the Kelihos botnet may incorrectly believe that Kelihos is the source of computer problems caused by the botnet. (Debenham Decl., ¶¶ 21-41.) Microsoft is similarly injured because the botnet directs an extraordinary amount of spam e-mail to users of Microsoft's e-mail services. (*Id.*) Microsoft and its customers must bear this extraordinary burden and customers may incorrectly believe that Microsoft is to blame for the spam e-mail. (*Id.*)

2. Kelihos' Unauthorized Intrusion Into Microsoft's Customers Computers

The most direct injury to Microsoft's customers is the installation of the Kelihos malware on their computers without their authorization or knowledge. (Debenham Decl., ¶¶ 25-32.) Kelihos malware is specifically designed to infect and run on computers equipped with the Windows operating system, which is licensed by Microsoft to end-users. (*Id.*, Exs. 4-6.)

End users' computers can become infected with Kelihos malware through a variety of mechanisms, including deceptive emails, email attachments or websites which include a downloader designed to download Kelihos to the user's computer.

The installation of Kelihos malware in and of itself damages the user's computer and the Windows operating system on the user's computer. (*Id.* ¶ 28.) During the infection of an end-user's computer, Kelihos malware makes changes at the deepest and most sensitive levels of the computer's operating system including the kernel, registry, and systems files. (*Id.*) It alters the behavior of various Windows operating system routines by manipulating various registry key settings. (*Id.*) It installs software that it needs to generate spam and to communicate with the Kelihos Command and Control Servers. (*Id.* ¶¶ 33-35) Microsoft's customers with computers infected with Kelihos malware are damaged by these changes to Windows that alter the normal and approved settings and functions of the user's operating system, destabilize it, and which result in the customers' computers being forcibly drafted into the botnet. (*Id.* ¶¶ 25-41)

Microsoft's customers are usually unaware of the fact that their computers are infected and have become part of the Kelihos botnet. (Debenham Decl., ¶¶ 20-24.) Even if aware of the infection, they lack the technical resources or skills to solve the problem, allowing their computers to be misused indefinitely. (*Id.*) Even with professional assistance, cleaning a botnet-infected end-user computer can be exceedingly difficult, time-consuming, and frustrating. (*Id.* ¶ 21.)

3. Kelihos Uses Microsoft Customer's Computers To Perpetuate Criminal Activity

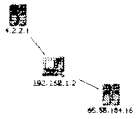
Once infected with Kelihos malware, the end-user's computer is under the control of the Defendants who use it for illegal activities. (Debenham Decl. ¶¶ 25-41.) The primary function of a Kelihos-infected end-user computer is to send out a very large quantity of illegal spam e-mail each day of its operation. (*Id.* ¶ 33.) Furthermore, the spam e-mails Kelihos-infected end-user computers disseminate illegal schemes and content. (*Id.* ¶¶ 37-40, Exs. 9-10.) Kelihos spam promotes pharmaceutical products that have been shown to be counterfeit, unlicensed,

and potentially dangerous to purchasers. (*Id.*) Kelihos spam promotes stock schemes, designed to artificially inflate stock prices. (*Id.*) In some instances, Kelihos spam advertise websites that purportedly offer pornographic and obscene material involving "minors" or individuals of "barely legal" age. (*Id.*) Customers are harmed by having their computers engaged in these illegal, harmful, and potentially criminal activities.

4. Microsoft Customers' Computer-Resources Are Utilized For Illicit Purposes

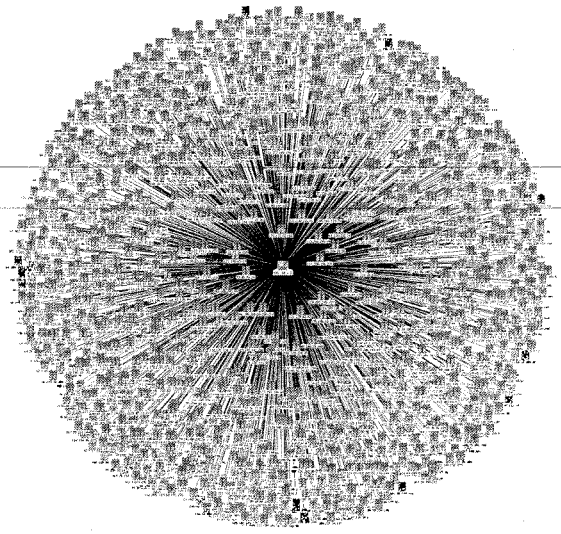
A Kelihos-infected end-user computer's processing power, memory, communications bandwidth, and other resources are used for the high volume of processing, data transfer and connections to the Internet that the Kelihos-infected end-user computer engages in. (Debenham Decl. ¶¶ 25-32.) For example, Figure 2 shows the tiny handful of Internet connections made by an uninfected Windows computer over the course of 6 hours. (*Id.* ¶ 31.)

Figure 2



In contrast, Figure 3, *infra*, shows the enormous number of Internet connections made over several hours by a Kelihos-infected end-user computer. *Id.* ¶ 32. The computing power and resources devoted to Kelihos' nefarious activities are unavailable for the customer's legitimate uses.

Figure 3



5. Kelihos Directly Targets Microsoft Customers

Kelihos' spam campaigns target Microsoft customers. (*Id.* ¶ 33.) For example, during one sample period, Kelihos-infected end-user computers revealed the capability of sending 94,560 spam e-mails each day and targeted more than 3,000 Hotmail accounts. (*Id.* ¶¶ 33-40.) The very large amount of spam reaching Microsoft's Hotmail customers frustrates them and diminishes their regard for Hotmail and Microsoft. (*Id.* ¶¶ 20-24.) Aside from the harm done to Microsoft Hotmail customers resulting from the sheer volume of Kelihos spam bombarding their Hotmail accounts, Kelihos' spam attempts to lure them into confidence schemes hatched by the spammers or other activities that will lead to further potential injury, such as purchasing counterfeit or unapproved pharmaceuticals on the Internet. (*Id.* ¶ 38.)

C. Kelihos Directly Injures Microsoft

1. Microsoft Pays The High Cost Of Dealing With Kelihos Spam

Microsoft, as a provider of online e-mail services such as Hotmail, must maintain spam filters to stop Kelihos spam from reaching its customers. (Debenham Decl. ¶ 21.) Kelihos has an estimated capacity to send 3.8 billion spam e-mails per day, including to users of Microsoft's Hotmail e-mail service. (*Id.* ¶ 33.) While the volume of spam attributed to Kelihos fluctuates over time, recent data shows that Kelihos is a substantial contributor of spam on the Internet. (*Id.*) Microsoft Hotmail systems are the target of a substantial volume of Kelihos spam. The sending of vast amounts of spam e-mail to Microsoft's Hotmail e-mail services imposes a burden on Microsoft's Hotmail systems, and requires Microsoft to expend substantial resources in an attempt to defend against and mitigate its effects. (*Id.* ¶¶ 21, 33.)

2. Microsoft Pays The High Cost Of Assisting Customers Whose Computers Are Infected By Kelihos

Additionally, Microsoft devotes significant computing and human resources to combating Kelihos infections and helping customers determine whether or not their computers are infected, and if so, cleaning them. (Debenham Decl. ¶ 21.) (estimating, conservatively, two person hours of effort to clean Kelihos off of a single computer). Customers' frustration

with having to deal with Kelihos infections on their computers diminishes their regard for Windows and Microsoft, and tarnishes Microsoft's reputation and goodwill. (*Id.* ¶¶ 20-24.)

D. Turning Off The IP Addresses And Domains Controlling The Kelihos Botnet Without First Informing The Defendants Is The Only Way To Prevent The Injury

Defendants, if given advance notice of any attempt to disable Kelihos by disconnecting the IP addresses and domains through which Kelihos operates, would take measures to keep Kelihos alive by migrating the command and control infrastructure to new IP addresses and domains. (Debenham Decl., ¶¶ 42-45; Kornblum Decl., ¶¶ 15-17.) Kelihos is designed to withstand technical counter-measures through various means:

a. it has an extensive Command & Control Tier, giving each Kelihos-infected end-user computer multiple points of contact with the botnet;

b. it changes the IP addresses of its Command and Control Servers over time; and

c. it provides the Kelihos-infected end-user computers with fallback domains.

Therefore, a piecemeal approach to disconnecting Kelihos' Command and Control Servers would fail. (*Id.*) If Microsoft disables less than all of the Command and Control Servers simultaneously and if any of the fallback mechanisms remain viable, the Kelihos-infected end-user computers will be able to migrate to the remaining Command and Control Servers to new IP addresses and domains. (*Id.*)

The only way to suspend the injury caused by Kelihos is to:

a. order the relevant hosting companies and IP registries to disable the IP addresses;

b. order Verisign and the domain registrars to disable the ".com" and ".cc" domains;

c. order that the content stored on the Command and Control Servers be made inaccessible and to disable any and all "backup" systems, arrangements or services;

d. order the hosting companies, registries and registrars suspend all services to the Defendants, to not warn or provide assistance to the Defendants, and to not enable any circumvention of the order;

Of particular importance is that the requested actions be closely coordinated, such that the malicious Command and Control IP addresses and domains, in various locations, are turned off simultaneously. (*Id.*) If there is delay between disabling Kelihos Command and Control Servers in the various locations, the Kelihos operators may become aware of this action, access the servers in the location that is delayed and move the botnet command and control tier to new, unidentified servers/locations. (*Id.*)

II. LEGAL ARGUMENT

Microsoft seeks an *ex parte* TRO and a preliminary injunction under Federal Rule of Civil Procedure 65(b), the All-Writs Act, 28 U.S.C. § 1651 and the court's inherent equitable authority to prevent compounding of the harm and to maintain the *status quo* by ensuring that the evidence of Defendants' misconduct is preserved during the pendency of this case. 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. *See Winter v. NRDC, Inc.*, 129 S. Ct. 365, 374-76 (2008); *Real Truth About Obama, Inc. v. Federal Election Com'n.*, 575 F.3d 342, 346-47 (4th Cir. 2009).

Microsoft is very likely to succeed on the merits. The Kelihos botnet's capacity to send billions of spam e-mails *each day*, the unlawful intrusion, and the deceptive use of Microsoft's brands violates the Computer Fraud & Abuse Act, the CAN-SPAM Act, and the Lanham Act. In addition, it is deceptive, misleading and tortious conduct in violation of Virginia and

Washington law. Microsoft, its customers, and the public will be irreparably harmed if the botnet continues to operate through the Harmful Botnet IP Addresses and Domains at issues in this motion.

By contrast, issuing the requested TRO and preliminary injunction will harm no legitimate interest of the Defendants. The purpose of the Harmful Botnet IP Addresses and Domains is to perpetuate the Kelihos botnet by disseminating malicious code that maintain and grows the botnet. That activity is itself unauthorized and is used to only further additional illegal activity. In addition, the public interest weighs very heavily in favor of relief because the same harm the botnet is causing to Microsoft and its customers is also imposed on many other U.S. computer users and companies as well. Accordingly, the relief Microsoft requests is warranted.

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

Microsoft is likely to succeed on the merits of its claims and as such, its request for a TRO and a preliminary injunction should be granted. 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 CAN-SPAM Act (15 U.S.C. § 7704), (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) trespass to chattels/computer trespass, (7) conversion, (8) unjust enrichment, and (9) negligence.

1. Defendants' Violations Of The Computer Fraud And Abuse Act

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

[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).

- 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 parties controlling the botnet intentionally access and send malicious code to Microsoft's and its customers' protected computers and operating systems, without authorization, in order to infect those computers and make them part of the botnet. The evidence submitted in support of this motion demonstrates that Microsoft and its customers are damaged by this intrusion. Performance of Microsoft's and its customers' computers is degraded due to the unauthorized intrusion, running of malicious code, collecting of personal information and carrying out of malicious conduct. Microsoft's Hotmail servers are burdened by the sending of an enormous amount of spam email to Microsoft's Hotmail accounts.

This is precisely the type of activity that the Computer Fraud and Abuse Act is designed to prevent. *See e.g. Physicians Interactive v. Lathian Systems, Inc.*, 2003 U.S. Dist. LEXIS 22868 (E.D. Va. 2003) (granting TRO and preliminary injunction under CFAA where defendant hacked into a computer and stole confidential information); *Global Policy Partners, LLC v. Yessin*, 2009 U.S. Dist. LEXIS 112472, *9-13 (E.D. Va. 2009) (accessing computer using credentials that did not belong to defendant actionable under the CFAA).[2] Indeed, some courts have aptly observed that the CFAA was targeted at "computer hackers (e.g., electronic trespassers)." *State Analysis, Inc. v. American Fin. Srvcs. Assoc.*, 621 F. Supp. 2d 309, 315 (E.D. Va. 2009) (citation omitted).

Further, spam emails sent by the Kelihos botnet to Hotmail users, burdening Microsoft's servers supporting that service and interfering with its goodwill, are actionable under the statute.

---

[2] Indeed, recent years botnet operators who disseminate code that intrudes upon user computers, collects personal information and causes injury have been indicted and convicted criminally under the Computer Fraud & Abuse Act. *See* Ramsey Decl., Exs. 14 (Indictment of Jeanson James Ancheta), 15 (Sentencing of Jeanson James Ancheta).

See e.g. America Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 451 (E.D. Va. 1998) (defendant's spamming in violation of plaintiff's terms of service violated CFAA); *Hotmail Corp. v. Van$ Money Pie Inc.*, 47 U.S.P.Q.2d 1020, 1025-26 (N.D. Cal. 1998) (granting preliminary injunction under CFAA where defendant sent spam email to Hotmail subscribers without their authorization). Similarly, here Microsoft is likely to succeed on the merits of its Computer Fraud & Abuse Act claim against the unlawful intrusion, collection of email addresses and other personal information, spam email and similar misconduct carried out by the botnet.

2. Defendants' CAN-SPAM Act Violations

The CAN-SPAM Act prohibits, among other acts, initiation of a transmission of a commercial electronic mail message "that contains, or is accompanied by, header information that is materially false or materially misleading." 15 U.S.C. § 7704(a)(1). Here, the Kelihos botnet automatically sends e-mails containing false "header" information (*i.e.* originating sender, IP address, etc.) making the e-mails appear to originate from addresses purporting to be associated with Microsoft, or other false addresses, thereby disguising their origin with the purpose of misleading recipients and evading detection. This is precisely what CAN-SPAM prohibits. *See Aitken v. Communs. Workers of Am.*, 496 F. Supp. 2d 653, 667 (E.D. Va. 2007) (inaccurate "from" line and header information may violate CAN-SPAM). Thus, Microsoft is likely to succeed on the merits of its CAN-SPAM Act claim.

3. Electronic Communications Privacy Act

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 so doing, obtaining, altering, or preventing authorized access to an electronic communication while it is in electronic storage. 18 U.S.C. § 2701(a). Microsoft's servers and its licensed operating system at end user computers are facilities through which electronic communication services are provided. The Kelihos botnet software, installed without authorization on infected computers, searches files such as emails and other files and steals personal email addresses and other information from those sources. Once harvested, these stolen

email addresses become targets for spam email or are used for other malicious purposes. 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). Thus, Microsoft is likely to succeed on the merits of its Electronic Communications Privacy Act claim.

4. False Designation Of Origin And Trademark Dilution

The Lanham Act 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 Kelihos botnet misleadingly and falsely causes the famous and distinctive Microsoft® and Windows® trademarks to be associated with malicious conduct carried out on users' computers through improper use of Microsoft's Windows operating system. Further, Defendants have misused the famous and distinctive Microsoft®, Windows®, Windows Live®, MSN® and Hotmail® trademarks in connection with the botnet domains. This conduct causes confusion and mistake as to Microsoft's affiliation with such misconduct and creates the false impression that Microsoft is the origin, when it is not. This activity is a clear violation of Lanham Act § 1125(a), thus Microsoft is likely to succeed on the merits. *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.)

The Lanham Act also 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, the Kelihos botnet's misuse of Microsoft's famous marks in connection with

malicious conduct aimed at Microsoft's customers and the public dilutes these famous marks by tarnishment and by blurring of consumer associations with the marks. Again, this is a clear violation of Lanham Act § 1125(c), and Microsoft is likely to succeed on the merits. *See e.g. America Online*, 24 F. Supp. 2d at 552 (spam email with purported "from" addresses including plaintiff's trademarks constituted dilution).

5. 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 and computers of customers interferes with and causes injury to the value of those properties. Thus, this conduct is an illegal trespass and also constitutes conversion. *See 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); *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."); *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 servers providing the Hotmail service, by sending Hotmail users vast quantities of spam e-mail, injures Microsoft's property and constitutes a trespass. *See e.g. 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*); *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.")

6. 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 parties controlling the botnet have taken the benefit of Microsoft's servers, networks and e-mail services, its licensed Windows operating system software and the computers of Microsoft's customers. Defendants have done so by improperly infecting these computers, and causing them to send and receive, collectively, an enormous volume of spam e-mails, including e-mail that infringes famous Microsoft trademarks. Defendants have profited from this activity. Thus, it is certainly inequitable for the parties controlling the botnet to retain this benefit. Microsoft is likely to succeed on the merits.

7. Negligence

The elements of a claim for negligence are (1) a duty of care, (2) a breach of that duty, (3) a showing the breach of that duty was the proximate cause of injury, (4) that results in damage to the plaintiff. *Blue Ridge Serv. Corp. of Va. v. Saxon Shoes, Inc.*, 271 Va. 206, 218, 624 (Va. 2006). A contract can impose a duty of care, a breach of which could give rise to a claim for negligence. *Davis v. Commonwealth of Virginia*, 230 Va. 201, 206 (Va. 1985) ("A legal duty is one either 'imposed by law, or by contract.'"); *Dunn Const. Co. v Cloney*, 278 Va. 260, 267 (Va. 2009). For example, the Defendants registered the domains through two domain registrars. When it did so, it agreed to the registrars' registration agreements that prohibited, among other things the use of the domains and associated services for any unlawful purpose or in violation of state, federal, or international law. (Ramsey Decl. Exs. 1 and 5.) In particular, the registration agreements prohibited (a) activities designed to encourage unlawful behavior by others; such as child pornography, (b) uploading material that would violate intellectual property rights; or (c) uploading, posting, or sending viruses or other computer code designed to interrupt, destroy or limit the functionality of any computer software or hardware. (*Id.*)

By agreeing to these terms, Defendants were subject to a duty of care to prevent this type of injury to third-parties, including Microsoft, which were reasonably foreseeable victims. Indeed, both through the terms of these contracts and generally under the law, Defendants, the owners and controllers of the botnet domains and IP addresses and the legally responsible parties for the domains and IP addresses, undertook affirmative obligations to prevent misuse of the domains. Accordingly, the Defendants were in a special relationship to any third party whom they allowed to use the domains and IP addresses to control the Kelihos botnet and carry out the misconduct alleged in this case. *See A.H. v. Rockingham Publ'g Co.*, 255 Va. 216, 220 (Va. 1998) (duty of care may arise where there is a special relationship between defendant and third party causing harm)

The Defendants carried out themselves and/or allowed third parties to use the domains and IP addresses to control, operate, and maintain the Kelihos Botnet. The Kelihos botnet

engages in the very unlawful conduct that is otherwise prohibited under the registration agreements. The Defendants, therefore, had a duty of care set forth under the law and by the registration agreements, which they breached by registering, using and/or allowing third parties to use the domains to control, operate, and maintain the Kelihos Botnet, and as a result, caused damage to Microsoft – namely the irreparable harm caused by the Kelihos botnet. The Defendants were negligent and Microsoft is likely to succeed on the merits.

B. Irreparable Harm Will Result Unless a TRO and Preliminary Injunction Are Granted

Continued operation of the Kelihos botnet irreparably harms Microsoft, its customers, and the public. No monetary remedy could repair the harm to Microsoft or its customers if the botnet were permitted to continue operating and expanding. Federal courts in civil cases addressing botnets have concluded that the "immediate and irreparable harm" to consumers from botnet command and control servers, spyware, viruses, Trojans, and phishing-related sites; and configuring, deploying and operating botnets, warranted an *ex parte* TRO and preliminary injunction. (*See* Ramsey Decl., Exs. 16-17 (*Microsoft Corporation v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va., Brinkema J.) (*Ex Parte* TRO and preliminary injunction to dismantle botnet command and control servers); Exs. 18-19 (*Microsoft v. John Does 1-11,* Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.) (*Ex Parte* TRO and preliminary injunction to dismantle botnet command and control servers); Exs. 12-13 (*FTC v. Pricewert LLC et al.*, Case No. 09-2407 (N.D. Cal. 2009) (Whyte J.) (*Ex Parte* TRO and preliminary injunction disconnecting service to botnet hosting company). Specifically, the district courts in *Microsoft Corporation v. John Does 1-27* and in *Microsoft Corporation v. John Does 1-11* acknowledged the substantial irreparable harm botnets cause Microsoft, its customers and Internet users generally. Ramsey Decl. at Exs. 16-17.

Microsoft and the public face the same irreparable harm caused by the Kelihos botnet. Thus, entry of an *ex parte* TRO disabling the Harmful Botnet IP Addresses and Domains and an Order to Show Cause why a preliminary injunction should not issue are warranted. Microsoft is irreparably injured because the problems of spam e-mail and system performance

degradation caused by the botnet are improperly attributed to Microsoft. Microsoft's customers may migrate to other platforms, products or services in the belief that Microsoft is the cause of the problems. Once such a switch occurs, given the costs of switching platforms and the uncertainty caused by the botnet in the first place, there is a very high risk that those customers will not return to Microsoft. As the botnet continues to grow, this harm is compounded. 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 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....").

Further, if the requested relief were not granted, the Kelihos botnet would continue to grow 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 or curtail the growth of the botnet. In the absence of the requested relief, Microsoft's customers would remain under constant threat of their computers being made part of the botnet with the accompanying 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 U.S. Dist. LEXIS 10847, *22 (M.D.N.C. 2007) (finding irreparable harm because defendant's actions "will have significant and continuous long-term effects.")

C. 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, because it will do nothing more than preserve the status quo. Disabling the Harmful Botnet IP Addresses and Domains through which the Kelihos botnet operates will prevent it from spreading to any additional computers during that time and will preserve the evidence of the botnet's structure and illegal activities. Defendants will suffer no harm if a TRO and preliminary injunction are issued because the Harmful IP Addresses and

Domains' purpose is to carry out illegal activity. (Debenham Decl. ¶ 18.) To the extent there is any legitimate activity carried out from and through the IP addresses and domains, such content, if any, can be easily and swiftly migrated to other IP addresses or separated technically from any botnet activity, through changes to DNS records or other technical means. (*Id.* ¶ 45.) 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 U.S. Dist. LEXIS 103688, * 10 (E.D. Va. 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 hosting companies, domain registries and domain registrars, as the requested relief is carefully tailored to only disable access to a small number of IP addresses and domains that they maintain and directs these third parties to take simple steps to assist in preserving evidence. The limited assistance sought from the third party hosting companies, domain registries and registrars is necessary to ensure effective implementation of the requested order and is authorized under the All-Writs Act, 28 U.S.C. § 1651.[3]

Conversely, if a TRO and preliminary injunction do not issue, the Kelihos botnet will continue to inflict irreparable injury on Microsoft, its customers, and the public. The botnet already includes approximately 41,000 compromised user computers, with the capability of sending billions of spam e-mails to Hotmail users each day. New users are infected each day,

[3] Federal courts also have the authority under the All-Writs Act, 28 U.S.C. § 1651 to order injunctive relief directing third parties to perform actions that are necessary to ensure effective implementation of court orders. *See United States v. New York Telephone Co.*, 434 U.S. 159, 174 (1977) (third party technical assistance required to implement order against Defendants); *In re Application of United States for an Order Authorizing An In-Progress Trace of Wire*, 616 F.2d 1122, 1129 (9th Cir. 1980) (same); *Eppley v. Mulley*, 2011 U.S. Dist. LEXIS 37094, *8-12 (S.D. Ind. 2011) (granting injunction against Defendants and directing third party internet service providers hosting or otherwise controlling websites to disable such websites, pursuant to All Writs Act).

dramatically increasing the botnet's capacity to carry out illegal conduct, compounding the injury to Microsoft and the public.

Simply put, maintaining the status quo by disabling the Harmful Botnet IP Addresses and Domains through which the botnet is controlled will not affect any legitimate rights of the Defendants, seeks only narrowly tailored assistance from the third-party hosting companies and domain registrars and registries, and will have a negligible effect on any potential legitimate interests of other third-parties. Allowing, however, the botnet to grow and continue to harm Microsoft and the public while this action is adjudicated poses grave danger to many legitimate interests.

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

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 with access to an email platform and the Internet is at risk of being irreparably injured by the Kelihos botnet. Similarly, every company providing email services and websites are at risk of having their systems misused to perpetuate the botnet. Indeed, there is specific evidence that the Kelihos domains are used to target malicious activity at not only Microsoft, but companies such as Google and Apple as well. Further, the spam email sent by the Kelihos botnet pushes fake and potentially dangerous pharmaceuticals, promotes fraudulent schemes that can injure consumers and promotes child pornography. (Debenham Decl., ¶¶ 18, 20-24) There is an overwhelming public interest in preserving the status quo and halting the growth of the Kelihos botnet while Microsoft proceeds with its claims.

This Court has 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 v. Lathian Systems, Inc.*, 2003 U.S. Dist. LEXIS 22868, *30 (E.D. Va. 2003) (granting TRO and preliminary injunction where defendant hacked into a computer and stole confidential information). More specifically, three district courts in the last

two years have concluded that "immediate and irreparable harm" will result to the welfare of consumers from "botnet command and control servers" and the malicious conduct carried out through botnets. (*See* Ramsey Decl., Exs. 16-17 (*Microsoft Corporation v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va., Brinkema J.); Exs. 18-19 (*Microsoft v. John Does 1-11,* Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.); Exs. 12-13 (*FTC v. Pricewert LLC et al.*, Case No. 09-2407 (N.D. Cal. 2009) (Whyte J.)). Specifically, the district courts in *Microsoft Corporation v. John Does 1-27* and in *Microsoft Corporation v. John Does 1-11* acknowledged the substantial irreparable harm botnets cause Microsoft, its customers and Internet users generally. Ramsey Decl. at Exs. 16-19. 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 criminals controlling the botnet will be able to continue their activities with impunity.

E. Only The Requested *Ex Parte* Relief Can Halt The Irreparable Harm To Microsoft And The Public

Absent a TRO granting the relief requested herein, the injury to Microsoft and the public, including Microsoft's customers, will continue unabated, irreparably harming Microsoft's reputation, brand and goodwill. The TRO, moreover, must issue *ex parte* for the relief to be effective at all, and the extraordinary factual circumstances here warrant such relief. 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, 94 S.Ct. 1113 (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*....").

1. If Notice Is Given, The Botnet Will Be Moved And Concealed, Allowing The Harm To Grow And Render Microsoft's Request For Relief Fruitless

If notice is given prior to issuance of a TRO, the Kelihos botnet Command and Control Servers will be moved to different servers, at different IP addresses and at different domains, in different areas, enabling Defendants controlling the botnet to continue infecting users' computers with malicious software, sending billions of spam e-mails and carrying out other conduct inflicting irreparable injury on Microsoft and the public. If the botnet's Command and Control Servers are allowed to move, the investigation of the botnet and the illicit activities carried out through it would have to be started anew. Providing notice of the requested TRO will undoubtedly facilitate efforts of the parties controlling the botnet to avoid prosecution.

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, *2 (D. Md. 2010) (granting an *ex parte TRO* where "Defendant may dissipate the funds and/or take action to render it difficult to recover funds....")[4]

There is specific evidence that operators of other botnets have attempted to evade prior enforcement attempts where they had notice, by moving the Command and Control Servers. Particularly instructive here is *Microsoft Corporation v. John Does 1-27* where, in February 2010, this Court issued an *ex parte* TRO and supplemental *ex parte* TRO suspending 276

[4] *Crosby v. Petromed, Inc.*, 2009 U.S. Dist. LEXIS 73419, *5 (E.D. Wash. 2009) (granting *ex parte* TRO as "notice to Defendants of this TRO request could result in further injury or damage to Plaintiffs...").

Internet domains used to control a malicious botnet. (*See* Ramsey Decl., Ex. 16 (*Microsoft Corporation,* Case No. 1:10-cv-156 (LMB/JFA) (E.D. Va., Brinkema J.)). 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 from 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 received advance notice of this action…

Id. at ¶4.

Moreover, in *FTC v. Pricewert LLC et al.,* the district court 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* Ramsey Decl., Ex. 12 (*FTC v. Pricewert LLC et al.*, Case No. 09-2407) (N.D. Cal., Whyte J.) at pg. 3.) Moreover, the court in *Dell, Inc. v. Belgiumdomains, LLC,* 2007 U.S. Dist. Lexis 98676, *4-5 (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, *inter alia*, using fictitious businesses, personal names, and shell entities to hide their activities. *Id.* at *4. In *Dell* the Court explicitly found that where, as in the instant case, Defendants' scheme is "in electronic form and subject to quick, easy, untraceable destruction by Defendants," *ex parte* relief is particularly warranted. *Id.* at *5-6.

2. If Notice Is Given, Evidence Regarding The Botnet Will Be Destroyed, Disturbing The Status Quo

If notice is given in advance of a TRO, evidence of the botnet will be destroyed. In particular, upon notice, the movement of the botnet command and control software will not only destroy evidence of the botnet's operation, but is also likely to lead to destruction of additional evidence available through that software, such as the identity of infected user

computers and other aspects of the system necessary to this litigation. 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 U.S. Dist. LEXIS 98676 at *4-5; *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.

F. 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.

Microsoft Will Provide Notice To The Defendants By Personal Delivery: Microsoft has identified 2 IP addresses and 21 domains from which the Kelihos command and control software operates, and, pursuant to the TRO, will obtain from the hosting companies and domain registrars/registries any and all physical addresses of the Defendants. Pursuant to Rules 4(e)(2)(A) and 4(f)(3), Microsoft plans to effect formal notice of the preliminary injunction hearing and service of the complaint by hand delivery of the summons, Microsoft's Complaint, the instant motion and supporting documents, and any Order issued by this Court to such addresses in the U.S., the Czech Republic and/or Switzerland. (Ramsey Decl., ¶¶ 11-16)

Microsoft Will Provide Notice To Defendants Through The Hague Convention On Service Abroad: Microsoft has identified the Piatti Defendants responsible for the "cz.cc" domains as residing in the Czech Republic and/or Switzerland. (Ramsey Decl., ¶¶ 2(a), 2(b)) Microsoft is prepared to effect notice of the preliminary injunction hearing and service of the complaint through the Hague Convention on the Service of Judicial and Extrajudicial Documents ("the Hague Convention") or other relevant judicial assistance treaties. (*Id.* ¶ 17)

Microsoft will translate the pleadings into the relevant language(s) and immediately request that the respective central authority deliver the summons, Microsoft's Complaints, the instant motion and supporting documents, and any Order issued by this Court to Defendants. (*Id.*)

Microsoft anticipates that this means of notice of the preliminary injunction hearing and service of the Complaint could take approximately three to six months to effect service through the respective central authorities. (Ramsey Decl., ¶ 17.) Accordingly, in addition to making every effort to expedite this process, given the irreparable harm and the need for prompt relief, Microsoft and its counsel will also provide notice of the TRO and the preliminary injunction hearing and will effect service of the Complaint through other means described below.

Microsoft Will Provide Notice By E-mail, Facsimile And Mail: Microsoft has identified email addresses, mailing addresses and/or facsimile numbers provided by the Defendants, and will further identify such contact information pursuant to the terms of the requested TRO. Microsoft will provide notice of the preliminary injunction hearing and will effect service of the Complaint by immediately sending the same pleadings described above to the e-mail addresses, facsimile numbers and mailing addresses that Defendants provided to the hosting companies in relation to hosting the command and control software at the Kelihos IP addresses and to the domain registrars/registries in relation to the Kelihos domains. When Defendants registered for domain names, they agreed not to engage in abuse such as that at issue in this case and agreed that notice of disputes regarding hosting could be provided to them by sending complaints to the e-mail, facsimile and mail addresses provide by them. (*See* Ramsey Decl., ¶¶ 2(c)-2(x), 3-10, 20-32.)

Microsoft Will Provide Notice To Defendants By Publication: Microsoft will notify the Defendants of the preliminary injunction hearing and the complaint against their misconduct by publishing the materials on a centrally located, publically accessible source on the Internet for a period of 6 months. Microsoft will also effect notice by additional methods including newspaper publication and other means as may be directed by the Court. (Ramsey Decl., ¶ 18)

Notice and service by the foregoing means satisfy Due Process, are appropriate, sufficient and reasonable to apprise Defendants of this action and are necessary under the circumstances. Microsoft hereby formally requests that the Court approve and order the alternative means of service discussed above.

First, legal notice and service by e-mail, facsimile, mail 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). Such methods are also 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, 1014-1015 (9th Cir. 2002) (authorizing service by e-mail upon an international defendant); Ramsey Decl., Ex. 16 (*Microsoft Corp. v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va. 2010, Brinkema J.)); *Smith v. Islamic Emirate of Afghanistan*, 2001 U.S. Dist. LEXIS 21712 (S.D.N.Y. 2001) (authorizing service by publication upon Osama bin Laden and the al-Qaeda organization); *FMAC Loan Receivables v. Dagra*, 228 F.R.D. 531, 535036 (E.D. Va. 2005) (acknowledging that courts have readily used Rule 4(f)(3) to authorize international service through non-traditional means); *BP Products North Am., Inc. v Dagra,* 236 F.R.D. 270, 271-73 (E.D. Va. 2006) (approving notice by publication); *AllscriptsMisys, LLC v. Am. Digital Networks, LLC,* 2010 U.S. Dist. LEXIS 4450, *3 (D. Md. 2010) (granting *ex parte* TRO and order prompting "notice of this Order and Temporary Restraining Order as can be effected by telephone, electronic means, mail or delivery services.").

Such service is particularly warranted in cases such as this involving Internet-based misconduct, carried out by international defendants, causing immediate, irreparable harm. As the Ninth Circuit recently observed:

> [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 e-mail-the method of communication which [Defendant] utilizes and prefers. In addition, e-mail 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, e-mail may be the only means of effecting service of process.

Rio Properties, Inc., 284 F.3d at 1014-1015[5]; *see also Williams-Sonoma, Inc. v. Friendfinder, Inc.*, 2007 U.S. Dist. LEXIS 31299, *5-6 (N.D. Cal. 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 provided by Defendants to the hosting companies and domain registrars, in the course of obtaining services that support the botnet, are likely to be the most accurate and viable contact information and means of notice and service. Moreover, Defendants will expect notice regarding their use of the hosting providers' and domain registrars' services to operate their botnet by those means, as Defendants agreed to such in their agreements. *See Nat'l Equip. Rental, Ltd. v. Szukhent,* 375 U.S. 311 (1964) ("And it is settled ... that parties to a contract may agree in advance to submit to the jurisdiction of a given court, to permit notice to be served by the opposing party, or even to waive notice altogether."). For these reasons, notice and service by e-mail and publication are warranted and necessary here.[6]

For all of the foregoing reasons, Microsoft respectfully requests that the Court enter the requested TRO and order to show cause why a preliminary injunction should not issue, and further order that the means of notice of the preliminary injunction hearing and service of the

---

[5] *Rio Properties* has been followed in the Fourth Circuit. *See FMAC Loan Receivables*, 228 F.R.D. at 534 (E.D. Va. 2005) (following *Rio*); *BP Prods. N. Am, Inc.*, 232 F.R.D. at 264 (E.D. Va. 2005) (same); *Williams v. Adver. Sex L.L.C.*, 231 F.R.D. 483, 486 (N.D. W. Va. 2005) ("The Fourth Circuit Court of Appeals has not addressed this issue. Therefore, in the absence of any controlling authority in this circuit, the Court adopts the reasoning of the Ninth Circuit in *Rio Properties, Inc.* ...)

[6] Additionally, if the physical addressees provided by Defendants to hosting companies turns out to be false and Defendants' whereabouts are unknown, the Hague Convention will not apply in any event and alternative means of service, such as email and publication, would be appropriate for that reason as well. *See BP Products North Am., Inc.*, 236 F.R.D. at 271 ("The Hague Convention does not apply in cases where the address of the foreign party to be served is unknown.")

complaint set forth herein meet Fed. R. Civ. Pro. 4(f)(3), satisfy Due Process and are reasonably calculated to notify Defendants of this action.

III. CONCLUSION

For the reasons set forth herein, 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: September 22, 2011 Respectfully submitted,

ORRICK, HERRINGTON & SUTCLIFFE LLP

REBECCA L. MROZ
Va. State Bar No. 77114
CHRISTOPHER M. O'CONNELL
Va. State Bar No. 65790
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
bmroz@orrick.com
coconnell@orrick.com

Of counsel:

GABRIEL M. RAMSEY (*pro hac vice* application pending)
JACOB M. HEATH (*pro hac vice* application pending)
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