IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

MICROSOFT CORPORATION, a Washington Corporation,

Plaintiff

v.

JOHN DOES 1-8 CONTROLLING A COMPUTER BOTNET THEREBY INJURING MICROSOFT AND ITS CUSTOMERS,

Defendants.

§
§
§
§
§
§
§
§
§
§
§
§
§
§
§

CASE NO: A13CV1014

FILED UNDER SEAL

APPLICATION OF MICROSOFT CORPORATION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

Plaintiff Microsoft Corp. ("Microsoft"), by counsel, pursuant to Federal Rule of Civil Procedure 65(b) and (c); the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the Electronic Communications Privacy Act (18 U.S.C. § 2701); the Lanham Act (15 U.S.C. §§ 1114, 1116, & 1125); the common law of trespass, conversion and unjust enrichment; and the All Writs Act (28 U.S.C. § 1651), respectfully moves the Court for an emergency *ex parte* temporary restraining order and order to show cause why a preliminary injunction should not issue.

As discussed in Microsoft's brief in support of this Application, Microsoft requests an order disabling a number of Internet Protocol (IP) addresses and Internet Domains by which Defendants control a harmful "botnet" known as the "ZeroAccess botnet." The ZeroAccess botnet is made up of close to two million end-user computers infected with malicious software that puts the infected computers under the control of Defendants, who use them for illegal activities, including "browser hijacking," "click-fraud," the theft of end-user's personal

identifying information, and infringing Microsoft's trademarks. The requested relief is necessary to halt the irreparable injury to Microsoft, its customers, and the public caused by the botnet. As discussed in Microsoft's brief in support of this Application, *ex parte* relief is essential because if Defendants are given prior notice, they will be able to destroy, move, conceal, or otherwise make inaccessible facilities through which Defendants direct the harmful ZeroAccess botnet. Therefore, Microsoft respectfully requests that the Court grant this Application.

Microsoft's Application is based on: this Application; Microsoft's Brief In Support Of This Application; the Declarations of David Anselmi, Jason Lyons, and Jacob M. Heath in support of Microsoft's Application and the exhibits attached thereto; the pleadings on file in this action; and on such argument and evidence as may be presented at the hearing on this Application.

Microsoft further respectfully requests oral argument on this motion to be set for November 25, 2013.

Dated: November 25, 2013

Respectfully submitted

FISH & RICHARDSON P.C.

By: _____

David M. Hoffman
Texas Bar No. 24046084
hoffman@fr.com

William Thomas Jacks
Texas Bar No. 10452000
jacks@fr.com

111 Congress Ave, Suite 810
Austin, TX 78701
Telephone: +1 (512) 472-5070
Facsimile: +1 (512) 320-8935 Fax

Of Counsel:

ORRICK, HERRINGTON & SUTCLIFFE LLP

Gabriel M. Ramsey
(*pro hac vice application pending*)
gramsey@orrick.com

Jeffrey L. Cox
(*pro hac vice application pending*)
jcox@orrick.com

Jacob M. Heath
(*pro hac vice application pending*)
jheath@orrick.com

Robert L. Uriarte
(*pro hac vice application pending*)
ruriarte@orrick.com

1000 Marsh Road
Menlo Park, California 94025
Telephone: +1 (650) 614-7400
Facsimile: +1 (650) 614-7401

Counsel for Plaintiff
MICROSOFT CORPORATION

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

I. INTRODUCTION

Plaintiff Microsoft Corp. ("Microsoft") seeks an emergency *ex parte* temporary restraining order ("TRO") and a preliminary injunction ordering Internet service providers in the U.S. to cut-off communication with 18 internet IP addresses in Europe that are being used by the cybercriminal operation known as the ZeroAccess botnet ("ZeroAccess"), which is harming consumers and businesses throughout the country, including within this judicial district.

Microsoft seeks relief under Federal Rule of Civil Procedure 65(b), the Lanham Act, 15 U.S.C. § 1116(a), 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 and to ensure that evidence of Defendants' misconduct is preserved during the pendency of this case.

Extraordinary relief is warranted because ZeroAccess causes extreme and continued irreparable harm to Microsoft, its customers, and the general public. If alerted in advance, Defendants will be able to hide their illegal operations and destroy critical evidence of their wrongdoing.

Botnets are vast networks of computers infected with malicious software ("malware") that transforms the computers into tools for criminal activity ranging from stealing personal information to defrauding businesses. Botnets harm nearly all users of the Internet, afflicting end users, corporations, and governments alike.

The ZeroAccess botnet has infected millions of end-user computers. For example, on just October 23, 2013, nearly 20,000 ZeroAccess-infected computers were active in Texas, many of those in the Austin metropolitan area. The malware downloads itself onto computers that connect to one of many websites set up or hacked by the Defendants. Once downloaded to the

victim's computer, the malware masquerades as a legitimate piece of software and deceives the victim into installing it. As ZeroAccess installs, it damages Microsoft Windows by disabling its security features, overwriting its drivers and altering its registry settings. ZeroAccess then cripples Internet Explorer and converts it into a counterfeit tool for cybercrime.

ZeroAccess also enlists the computer into an army of infected computers that Defendants control through a set of servers based in Europe. These malicious servers are connected to the Internet through the 18 Internet Protocol ("IP") addresses and 49 Internet domains that Microsoft has identified in Appendix A. These 18 IP addresses and 49 domains are the express conduit by which Defendants inflict injury and control their victim computers within the United States.

The infected computer serves as a tool for crime for Defendants, who use it to steal money by defrauding online advertising systems. Because its security defenses are disabled, the computer is vulnerable to secondary malware infections. These include Zeus, an infamous financial fraud botnet that spies on the owner's online banking activities and then uses that information to empty the accounts, as well as other types of malware-driven scams.[1]

ZeroAccess causes severe injury to Microsoft's reputation and goodwill. It corrupts and thereby alters the normal operation of Microsoft's Windows® operating system, Internet Explorer® browser and Bing® search engine, essentially converting those widely used applications, complete with the well known Microsoft marks, into counterfeit tools for fraud. It also reduces the performance of infected computers running Microsoft's Windows operating system, a loss of performance customers often attribute to problems with Windows itself.

The requested TRO directs the disablement of communications between the computers infected with ZeroAccess and the IP addresses (the "Fraud Control IP Addresses") and domains

[1] According to conservative estimates by researchers, cybercriminals have exfiltrated over 100 million dollars through Zeus.

(the "Fraud Control Domains") through which the infected computers receive instructions on how to commit the fraud that is the daily stock-in-trade of ZeroAccess. At each Fraud Control IP Address, Defendants have connected one or more specialized computers (the "Fraud Control Servers") which communicate those instructions to the infected computers. Disabling communications through the ZeroAccess Fraud Control IP Addresses and Domains will cut communication between the infected computers and the Defendants. Once the ZeroAccess Fraud Control Servers cannot communicate with the infected end-user computers, Defendants will no longer be able to instruct those infected end-user computers on browser hijacking and click fraud.

Ex parte relief is essential here as notice to Defendants would provide them an opportunity to destroy, move, conceal, or otherwise make inaccessible the instrumentalities used to direct ZeroAccess—the primary evidence of their unlawful activity. If given notice, it is virtually certain that Defendants will shift their fraud control infrastructure before the relief sought in the TRO is afforded and/or adapt the botnet to make it more difficult to disrupt the browser hijacking and click fraud control infrastructure and to initiate the notification and remediation process for the infected computers. The proposed order sought herein will block the current 18 Fraud Control IP Addresses and 49 Fraud Control Domains and would authorize Microsoft to supplement the order with new IP addresses or domains, should the defendants attempt to evade the order by using new IP addresses or domains.

The requested *ex parte* relief is not uncommon when disabling dangerous botnets, as courts in seven cases involving Microsoft and other plaintiffs have granted such extraordinary relief to disable botnets. For example, in the February 2010 case concerning the "Waledac" botnet, the District Court for the Eastern District of Virginia (Judge Brinkema) adopted an

approach where:

1. the Court issued a tailored *ex parte* TRO, including provisions sufficient to effectively disable the harmful botnet infrastructure, preserve all evidence of its operations and stop the irreparable harm being inflicted on Microsoft and its customers;
2. immediately after implementing the TRO, Microsoft undertook a comprehensive effort to provide notice of the preliminary injunction hearing and to effect service of process on the defendants, including Court-authorized alternate service by email, electronic messaging services, mail, facsimile, publication, and treaty-based means; and
3. after notice, the Court held a preliminary injunction hearing and granted the preliminary injunction while the case proceeded in order to ensure that the harm the botnet cause would 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 Jacob M. Heath ("Heath Decl."), Exs. 14 and 15.) Subsequently, in six other cases involving dangerous botnets, Federal Courts have followed this approach. *See Microsoft v. John Does*, 1-11, Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.) (at Heath Decl., Exs. 16 and 17; involving the "Rustock" botnet); *Microsoft v. Piatti, et al.*, Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.) (Heath Decl., Exs. 18 and 19; involving the "Kelihos" botnet); *Microsoft Corp. et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.) (Heath Decl. Exs. 20 and 21; involving the "Zeus" botnets); *Microsoft Corp. v. Peng Yong et al.*, Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.) (Heath Decl., Ex. 22; involving the "Nitol" botnet); *Microsoft Corp. v. John Does 1-18 et al.*,

Case No. 1:13-cv-139-LMB/TCB (E.D. Va.) (Brinkema, J.) (Heath Decl. Exs. 30 and 31; involving the "Bamital" botnet); *Microsoft v. John Does 1-82*, Case No. 3:13-CV-00319-GCM (W.D.N.C.) (Mullen, J.) (Heath Decl. Exs. 32 and 33; involving the "Citadel" botnets).

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

II. FACTUAL BACKGROUND: THE ZEROACCESS BOTNET

"ZeroAccess—also known as "Sirefef" or "max++"—is malicious software ("malware") that surreptitiously infects users' computers and, without the user's knowledge, and assimilates their computers into a network of computers known as a "botnet." (Declaration of David Anselmi ISO TRO ("Anselmi Decl.") ¶ 3) Recent counts found approximately 1.9 million infected computers world-wide, with as many as 800,000 of those active in fraud operations on any given day. (*Id.* ¶ 3) Most infected computers are located within the United States and Western Europe. Recently, Microsoft detected approximately twenty-thousand infected computers in Texas in a single day. (*Id.* ¶ 3)

Botnets in general provide a very efficient means of controlling large numbers of computers and targeting any action internally against the contents of those computers or externally against other computers on the Internet. (*Id.* ¶ 39) The botnet operators can use the network of infected personal computers for various nefarious and criminal activities including spam, denial of service attacks on other computers connected to the Internet, theft of financial and banking data, eavesdropping, stalking, and other schemes. (*Id.* ¶ 39) Access to the

compromised personal computers can also be sold, leased, or swapped by one criminal group to another. (*Id.* ¶ 39)

Microsoft's investigation has shown that cybercriminals operating the ZeroAccess botnet use the infected computers to engage in various forms of illegal activity relating to online advertising fraud, including "browser hijacking." and "click-fraud."[2] (*Id.* ¶ 5) Through browser hijacking, the cybercriminals operating ZeroAccess can connect the infected computers to unsafe websites at will. (*Id.* ¶ 5) They are able to monetize this by selling the resulting traffic to websites that host advertisements as part of online advertising platforms. However, sometimes the website purchasing the traffic is owned by other cybercriminals, who purchase traffic generated by ZeroAccess as a way to spread their own malware. Through click fraud, Defendants are able to direct infected computers to go to websites of their choosing and simulate clicks on advertisements there, making ZeroAccess-generated traffic even more valuable to websites seeking to earn money through online advertising.

A. Online Advertising And Fraud

The multibillion dollar online advertising ecosystem is a lucrative target for fraud due to its rapid growth, size, and complexity. (*Id.* ¶¶ 10-11) Cybercriminals have devised multiple schemes to manipulate the online advertising business model, siphoning off millions of dollars annually. (*Id.* ¶ 11) For example, cybercriminals have devised multiple techniques to fake "clicks" on or views of advertisements, events that generate revenue for the website hosting the advertisement that was clicked on or viewed. (*Id.* ¶ 11) Cybercriminals do so by infecting

[2] ZeroAccess also includes a module for "bitcoin mining." Bitcoin is an unregulated electronic cryptographic currency used frequently by cybercriminals. Bitcoin mining involves computing extremely large equations in order to "find" new bitcoins. Defendants harness the combined processing power of the multitude of computers that comprise the ZeroAccess botnet in order to supplement the income derived from click fraud and browser hijacking.

victim computers with malicious software, commonly referred to as "malware" which causes the victim computers to make such "clicks" without the consent of the computer's owner. (*Id.* ¶ 12) This scheme works well for cybercriminals, as a very large number of geographically dispersed victim computers can generate fake clicks in low enough volumes, per computer, that the activity can evade fraud control systems put in place by advertising platforms being defrauded. (*Id.*)

Microsoft provides one of the predominant online advertising platforms on the Internet and is therefore a target of online fraud. Microsoft owns and operates the Bing® search engine and an online advertising platform called Microsoft Bing® Ads. (*Id.* ¶ 13) As part of its Bing Ads business, Microsoft contracts with various companies who wish to place advertisements on the Internet ("Advertisers"). (*Id.* ¶ 13) Microsoft places the Advertisers' advertisements on, among other places, a network of websites published by other entities or individuals ("Publishers") that also participate in Microsoft's advertising network program.

In general, the idea is that users click on advertisements of interest and takes additional actions, such as purchasing and Advertiser's products or services. (*Id.* ¶ 14) When a user clicks on an advertisement, the Advertiser pays the Publisher of the website where the click occurred. (*Id.* ¶¶ 15-16). Unfortunately, malicious actors use end-user computers infected with malware, automated scripts, or other schemes to generate a large number of clicks on and/or views of the advertisements placed on websites by Microsoft's Bing Ads and similar platforms. (*Id.* ¶ 17) The advertisers and Microsoft are injured by this fraudulent activity, because the advertiser pays for "clicks" that do not reflect a real user with any real interest in the product or service being advertised. (*Id.* ¶¶ 17-21) This activity is termed "click-fraud." (*Id.* ¶ 17)

In the case at hand, Defendants have infected end-user computers malware and recruited them into the ZeroAccess botnet. The ZeroAccess malware is surreptitiously installed on victim

computers in order to carry out "search hijacking" and "click fraud," to defraud Microsoft and online advertisers. ZeroAccess forces visits to websites and clicks on advertisements in order to fraudulently generate money through abuse of Microsoft's Bing Ads platform and other prominent advertising platforms and advertisers. (*Id.* ¶ 20)

B. ZeroAccess Malware Is Installed On Victim Computers Through Misleading Schemes And Without Consent

ZeroAccess is installed on victim computers through misleading schemes. The majority of ZeroAccess infections result from what are known as "drive-by-downloads." (*Id.* ¶ 43) In a drive-by-download, a cybercriminal creates or hacks a website and stages on that website specialized software known as an "exploit pack" designed to infect end user computers. (*Id.* ¶ 43) These websites are known as "exploit websites." (*Id.* ¶ 43) When a user's computer connects to such a website, the exploit pack silently probes the user's computer, looking for unpatched vulnerabilities in the operating system or in third-party applications, or the absence of an updated anti-virus program, that would provide an opportunity to execute code or hook malware into the operating system. (*Id.* ¶ 43) If the exploit pack finds an un-patched vulnerability or the absence of an updated anti-virus program, it downloads and installs the ZeroAccess malware or other malware onto that computer. (*Id.* ¶ 43)

To bring users to the exploit website, the cybercriminal will typically plant redirector code on other websites on the Internet. (*Id.* ¶ 44) These may be popular websites that the cybercriminal has hacked specifically for this purpose, or websites specially designed to lure the unsuspecting and then redirect them to the exploit website. (*Id.* ¶ 44) When an unsuspecting user browses to one of these websites, the redirector code on the website automatically and surreptitiously causes the user's computer to be connected to the exploit website. (*Id.* ¶ 44) Once infected, the user's computer becomes part of the botnet, able to communicate with and

receive instructions from the botnet's operators as described in detail below, giving the botnet operators control over the user's computer. (*Id.* ¶ 46)

C. ZeroAccess Damages The Windows Operating System And Internet Explorer During Installation

ZeroAccess malware needs administrator access privileges to install itself. In most cases, to acquire that level of access, it will seek to fool the user into allowing it to run with that level of access. (*Id.* ¶ 47) It does this by pretending to be a legitimate upgrade for software on the user's computer, and by fooling the user into launching the false, counterfeit "upgrade" as an administrator. (*Id.* ¶¶ 47-48) Once able to install, ZeroAccess makes damaging changes to the Windows operating system and to Internet Explorer. (*Id.* ¶ 49) It creates hidden directories, overwrites software drivers needed by the operating system, injects itself into low-level processes, and makes changes to the system registry, which is a primary repository of crucial information the computer needs to run correctly. (*Id.* ¶ 49) It also injects code in the Internet Explorer process, effectively converting Internet Explorer into a malware program which, though still bearing the name Internet Explorer, instead becomes a counterfeit instrument of fraud. (*Id.* ¶ 49)

One of the most dangerous changes that ZeroAccess makes to an infected computer is to disable its defenses, lowering security credentials and disabling Windows security services. (*Id.* ¶ 50-52) The ZeroAccess malware, by disabling these services, keeps infected computers from, among other things, installing security updates from Microsoft. It disables the following Windows services: Base Filtering Engine Service, IP Helper service, Windows firewall service, Windows Defender service, Windows Security Center Service), and Proxy Auto Discovery Service. (*Id.* ¶ 50) This is particularly dangerous because ZeroAccess repeatedly connects the infected computer to websites from which other malware may attack it. With Windows security

features disabled, the computer owner has little chance of avoiding a rash of secondary infections, some of which are exceedingly dangerous.

D. The Architecture Of The ZeroAccess Botnet

1. ZeroAccess Is A World-Wide Network Of Infected Computers Designed To Resist Countermeasures

In general, the Defendants have designed and deployed ZeroAccess using what is known as a "peer-to-peer" network topology. (*Id.* ¶ 36) This architecture is employed as a way to resist countermeasures. (*Id.* ¶¶ 35-36) In a peer-to-peer network, the participating infected computers, called "nodes," or "peers," engage in constant communication with each other, and can quickly and reliably update each other with new versions of the malware and new instructions. (*Id.* ¶ 36) In other words, in a peer-to-peer network, any one of the infected computers can function as a command-and-control server. (*Id.* ¶ 36) Consequently, there is no single point of command and control that provides an easy target for those seeking to disrupt the entire network. (*Id.* ¶¶ 36-37) In fact, it recently withstood and quickly recovered from an attempt made by a major security software company to neutralize it. (*Id.* ¶ 37) Indeed, following this recent attempt to stop it, the cybercriminals behind ZeroAccess added additional layers of redundancy to the peer-to-peer network, making it even harder to disrupt, much less eradicate. (*Id.* ¶¶ 37, 53-54)

2. Defendants Control ZeroAccess Through 18 IP Addresses Based In Europe

Notwithstanding the resilience of the peer-to-peer network, generally, the architecture of ZeroAccess is vulnerable in that the infrastructure that controls the click fraud or browser hijacking is a discrete and relatively static set of IP addresses. The infected computers in the peer-to-peer network rely on this separate set of servers located at 18 IP addresses maintained by Defendants at hosting companies in Latvia, Luxembourg, Switzerland, the Netherlands, and Germany. (*Id.* ¶¶ 55-56) When ZeroAccess first infects a computer, it does not contain the files

or modules required to commit actual click fraud or browser hijacking. (*Id.* ¶ 55) Instead, it must acquire these from the first peer it contacts. (*Id.* ¶ 55) Each time a ZeroAccess-infected computer contacts any other peer, it also asks what other ZeroAccess modules or files that peer has. (*Id.* ¶ 55) The files that a ZeroAccess-infected computer will acquire in this fashion contains a list of IP addresses of servers that are not part of the peer-to-peer network, but which instead give the infected computer explicit instructions on how to commit the click fraud or browser hijacking. (*Id.* ¶ 56) This list of IP addresses changes gradually over time, but currently there are 18 of them. (*Id.* ¶ 56) These "Fraud Control IP Addresses" are listed in Appendix A. (*Id.* ¶ 56) Disabling these IP addresses will disable the click fraud and search hijacking functionality, described further below. Further, these IP addresses are associated with 49 "Fraud Control Domains," believed to be fallback infrastructure, also listed in Appendix A.

E. Defendants Use ZeroAccess To Conduct Illegal Online Advertising Fraud

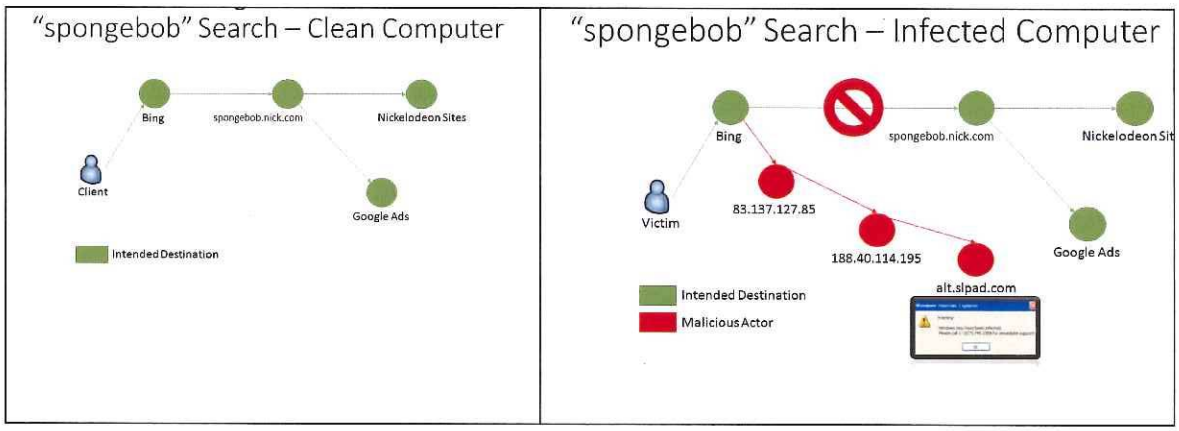
1. ZeroAccess Browser Hijacking Fraud

One of the major frauds that Defendants perpetrate though ZeroAccess is browser hijacking. Browser hijacking operates as follows: First, through a web browser such as Internet Explorer, the user uses a search engine, for example Bing, Yahoo! or Google, to search for a particular topic. (*Id.* ¶ 58) The search engine returns a list of results, and the user reviews the links and determines which to click on. (*Id.* ¶ 58) As soon as the user clicks on one of the links, the ZeroAccess malware running on the user's computer redirects their browser to a computer server at one of the Fraud Control IP Addresses and transmits to that server the search terms that the user used in their search. (*Id.* ¶ 58) With that information, the command and control server redirects the user's computer it to one of numerous possible websites chosen by the botnet operators, all the while misrepresenting to the user that they are using the Bing-branded search engine containing Microsoft's Bing trademark and the Internet Explorer-branded browser. (*Id.* ¶

58) The following are examples of deceptive schemes carried out by the Defendants through ZeroAccess search hijacking:

Fake Customer Service Scam: The ZeroAccess search hijacking functionality is used to scam customers into paying for fake customer service. For example, Figure 1, below, shows the differing results for a user who searches for the term "spongebob" (an animated children's character) on a clean computer, versus on a ZeroAccess-infected computer. (*Id.* ¶ 58)

Fig. 1

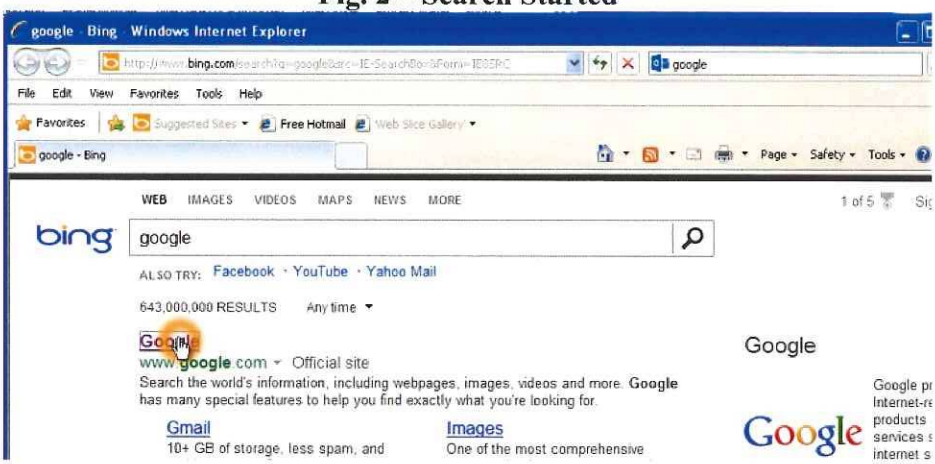


On the clean computer, the browser connects to the website "spongebob.nick.com," and then downloads further information from Nickelodeon sites and advertisements provided from Google's ad network. (*Id.* ¶ 58) On a ZeroAccess infected computer, however, the browser is hijacked and is sent first to two unnamed computers IP address on the Internet, and from there is connected to a website called "alt.slpad.com." (*Id.* ¶ 58) The error message that pops up at that point, notifying the user that the computer has been infected, is part of a scam. (*Id.* ¶ 58) If the user calls that number, the people responding will attempt to trick the user into paying to have their computer "cleaned." (*Id.* ¶ 58)

"Scareware" Fake Antivirus Scam: The ZeroAccess search hijacking functionality is used to direct customers to a form of malicious program known as "scareware," which is fake

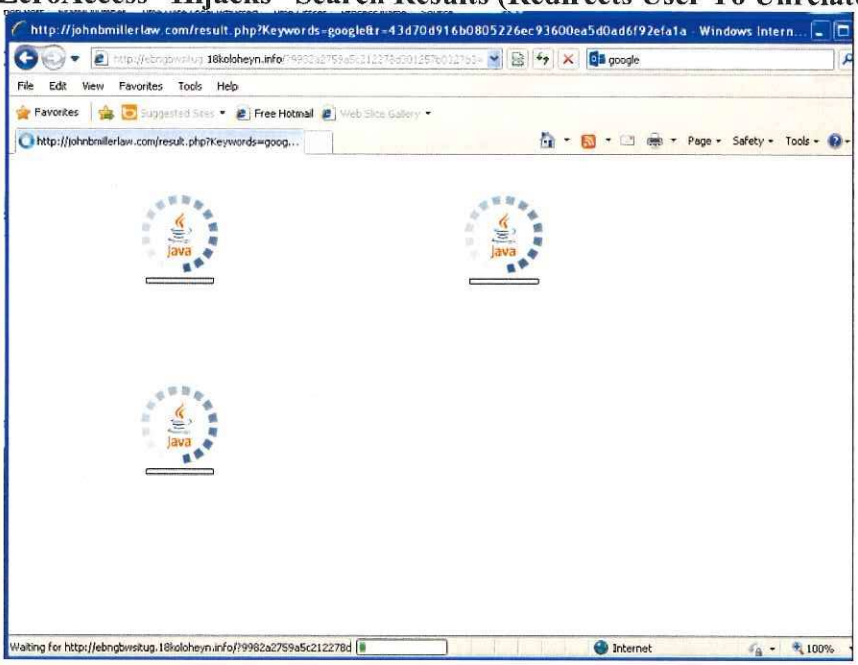
antivirus software designed to cause customers to provide their credit card information. Figures 2-4, below, illustrate a typical scareware scam carried out by Defendants through ZeroAccess. (*Id.* ¶ 62) First, the user uses the Microsoft Bing search engine to search for the term "Google." Bing returns the correct result, and the user clicks on the top link, expecting to go to Google. (*Id.* ¶ 62)

Fig. 2 – Search Started



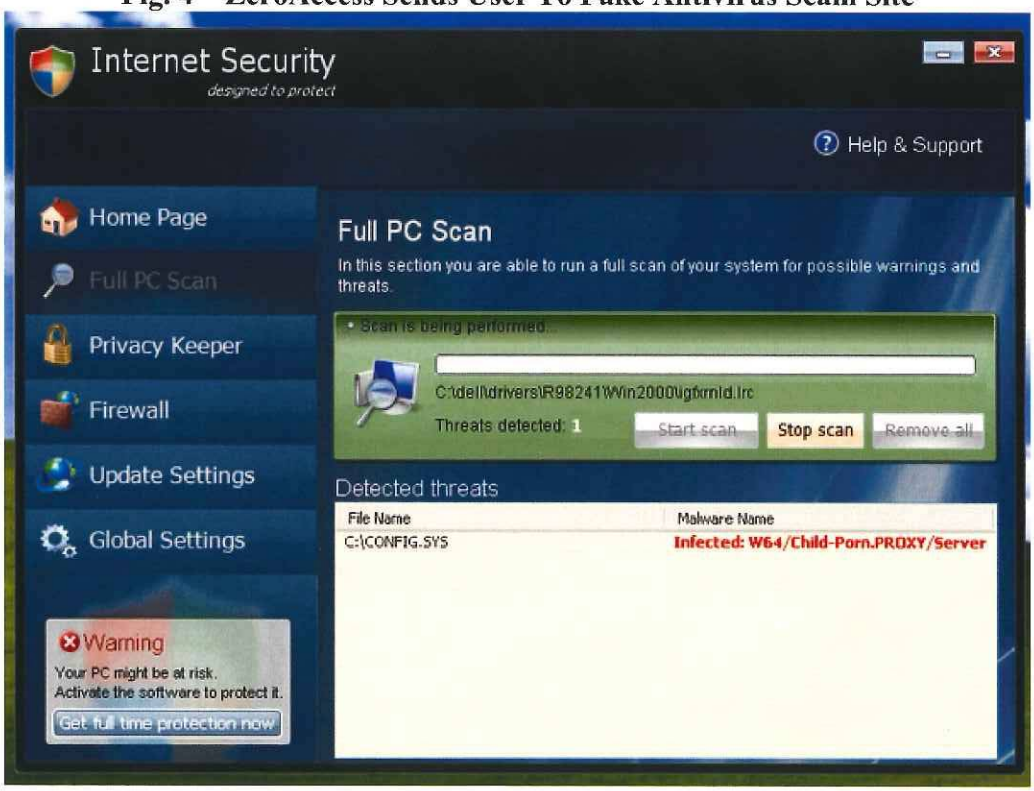
Instead of being connected to Google.com, the browser connects to a series of unrelated sites:

Fig. 3 – ZeroAccess "Hijacks" Search Results (Redirects User To Unrelated Sites)



Suddenly, the scareware launches on the user's computer, from the site that ZeroAccess redirected the user's browser. (*Id.* ¶ 62) The scareware pretends to have launched a security scan of the user's computer (in fact, no scan is being conducted), and to have found a threat related to child pornography. (*Id.* ¶ 62) The goal of this malware is to induce the user to click on the button in the lower left to "Get full time protection now." (*Id.* ¶ 62) Typically, this type of scam ends with an attempt to coax the user into making a credit card payment in order to get the "full-time protection." (*Id.* ¶ 62) In the meantime, the computer is effectively unusable—there is no way for the user to get rid of the fake security scan message without great time and effort. (*Id.* ¶ 62)

Fig. 4 – ZeroAccess Sends User To Fake Antivirus Scam Site



Financial Theft Malware: The ZeroAccess search hijacking functionality is also used to direct customers to websites that deliver further malicious code, designed to intercept their online

banking credentials and steal their money. In particular, Microsoft's investigation reveals that users are redirected by ZeroAccess to websites that then download the "Zeus" malware to their computers. (*Id.* ¶ 64) Zeus is a financial fraud botnet that spies on the owner of the computer and steals their financial account information, including identification information, account numbers, account balances, and passwords for online banking. (*Id.* ¶ 64) The criminals behind Zeus then use this information to surreptitiously empty the victim's bank account. (*Id.* ¶ 64) In December 2012, Microsoft and other plaintiffs from the financial industry won a default judgment against the operators of Zeus in the matter *Microsoft Corp. et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.), taking down significant portions of that botnet. (*Id.* ¶ 64) In spite of these concerted efforts and successes, branches of the Zeus botnet live on, and the operators of Zeus are evidently using ZeroAccess-generated traffic to infect more computers in an attempt to rebuild their criminal enterprise. (*Id.* ¶ 64)

2. ZeroAccess Click Fraud

A second main illegal activity engaged in by ZeroAccess-infected computers is click fraud. (*Id.* ¶ 65) When ZeroAccess-infected computers are turned on, the ZeroAccess malware running on those computers will connect with one or more of the 18 IP addresses listed in Appendix A. (*Id.* ¶ 65) The computers at those IP addresses provide the ZeroAccess-infected computer with a list of website addresses. (*Id.* ¶ 65) When a ZeroAccess-infected computer connects to one of the websites in the list, the hijacked computer's browser simulates a click on an advertisement at the website. (*Id.* ¶ 65) It then moves on to the next website in its list and repeats the process. (*Id.* ¶ 65)

The ZeroAccess click fraud takes advantage of the fact that online advertisers typically pay fees per click and a share of this revenue is paid to the website hosting the advertisement. In practice, a website operator pays the Defendants to have its website added to the list of addresses

that ZeroAccess's army of hijacked computers visit each day, or Defendants may control such websites directly and receive payment from an advertising network. The hijacked computers then visit those websites and click on the ads, which fraudulently makes it appear that legitimate consumers are clicking on and thus viewing those advertisements. The advertisers and the company, such as Microsoft, providing the ads then pay the website operator for the fraudulent clicks – falsely believe that they were legitimate consumers.

F. ZeroAccess Directly Damages Microsoft And Its Customers

1. ZeroAccess Damages Infected Computers

As noted above, ZeroAccess makes damaging changes to the Windows operating system. (*Id.* ¶ 68) It creates hidden directories, overwrites software drivers needed by the operating system, injects itself into low-level processes, and makes changes to the system registry, which is a primary repository of crucial information the computer needs to run correctly. (*Id.* ¶ 68) It also disables security features on the infected computer, lowering security credentials and disabling Windows security, leaving the computer susceptible to secondary infections. (*Id.* ¶ 69) It disables Base FilteringEngine Service, IP Helper service, Windows firewall service, Windows Defender service, Windows Security Center Service, and Proxy Auto Discovery Service. (*Id.* ¶ 69) The ZeroAccess malware, by disabling these services, keeps infected computers from, among other things, retrieving security updates from Microsoft. (*Id.* ¶ 69) These events take place without the knowledge or authorization of the end-user, as ZeroAccess runs as a background process (that is, it runs in the background, has no user-interface, and gives the computer's owner no indication that it is present or running). (*Id.* ¶ 69) As shown above, the fact that ZeroAccess disables a computer's defenses is particularly dangerous in that ZeroAccess also connects the user's computer to multiple websites from which the computer may be attacked by secondary malware infections. (*Id.* ¶ 69) Further, as described above, ZeroAccess injects

code in the Internet Explorer process, effectively converting Internet Explorer into a malware program which, though still bearing the name Internet Explorer, instead becomes a counterfeit instrument of online fraud, hijacking Internet searches carried out on a user's computer. (*Id.* ¶ 70)

Because of the operations described above, a ZeroAccess-infected end-user computer's processing power, memory, communications bandwidth, and other resources will be used for the high volume of processing, data transfer and connections to the Internet that the ZeroAccess-infected end-user computer engages in. (*Id.* ¶ 71) Users have reported computer performance degradation that has been attributed to ZeroAccess malware. (*Id.* ¶ 71)

Owners of ZeroAccess-infected computers are typically unaware that their machines are infected and operating as part of a ZeroAccess botnet, or that their computers are secretly engaged in illegal activity. (*Id.* ¶ 72) The ZeroAccess malware is designed to be hidden. Users that become aware that ZeroAccess is wrongfully installed on their system must expend time and experience frustration in an attempt to remove ZeroAccess from their systems. (*Id.* ¶ 72) Indeed, given the way that ZeroAccess installs itself, users attempting to clean it from their system unassisted run the risk of causing their browsers or computers not to operate correctly. (*Id.* ¶ 72)

2. ZeroAccess Irreparably Harms Microsoft And Its Brand

ZeroAccess irreparably harms Microsoft by damaging its reputation, brands, and customer goodwill. (*Id.* ¶ 73) Microsoft is the provider of the Windows operating system, Internet Explorer, Bing, Bing Ads, Hotmail e-mail service, and a variety of other software and services. (*Id.* ¶ 73) Microsoft has invested substantial resources in developing high-quality products and services. (*Id.* ¶ 73) 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. Microsoft has registered trademarks representing the quality of its products and services and its brand, including the Windows, Internet Explorer, and Bing marks. (*Id.* ¶ 73)

The activities of ZeroAccess injure Microsoft and its reputation, brand, and goodwill because users subject to the negative effects of these malicious applications incorrectly believe that Microsoft, Windows, Internet Explorer, Bing, or Bing Ads are the sources of their computer problems. (*Id.* ¶ 74) For example, because of ZeroAccess, users get less relevant and often harmful or dangerous search results, as their browser and the Bing search engine are hijacked to less relevant, dangerous or offensive sites. (*Id.* ¶ 74) There is a great risk that end-users may attribute these problems to Microsoft, Internet Explorer, Bing search engine or Bing Ads products, thereby diluting and tarnishing the value of these trademarks and brands. (*Id.* ¶ 74)

Customers may, and often do, incorrectly attribute the negative impact of the ZeroAccess botnet and other malware downloaded to their computers as a result of having their browsers hijacked and redirected to malware download sites to Microsoft. (*Id.* ¶ 76) Further, there may be significant challenges to having such customers return, given the cost they bear to switch to new products and perceived risks. (*Id.* ¶ 76)

Microsoft devotes significant computing and human resources to combating ZeroAccess and other malware infections and helping customers determine whether or not their computers are infected, and if so, cleaning them. (*Id.* ¶ 77) Not only does Microsoft expend resources in helping end-users combat ZeroAccess, it must also expend resources in monitoring its online advertising platform for fraudulent traffic and clicks, filtering them out before they do damage

where possible, and reimbursing advertising customers where it is discovered after the fact. (*Id.* ¶ 77) These efforts require in-depth technical investigations and extensive efforts to calculate and remediate harm caused to Microsoft's advertising customers. (*Id.* ¶ 77)

Microsoft and its customers are injured when the ZeroAccess botnet software and other malware is maliciously introduced onto people's computers making them part of the botnet. (*Id.* ¶ 78) The installation of the botnet software by deceiving consumers is an intrusion into and corruption of the Microsoft Windows operating system, without Microsoft's authorization. (*Id.* ¶ 78) The Windows operating system is licensed by Microsoft to its customers. (*Id.* ¶ 78)

3. ZeroAccess Damages Microsoft's Advertising Platform And Its Customers That Use It

a. ZeroAccess Causes Advertisers On Microsoft's Platform To Pay For Fraudulent Clicks

ZeroAccess also adversely affects Microsoft's advertiser customers, other advertisers and website owners, who legitimately pay service providers such as Bing Ads to increase targeted traffic to their website. (*Id.* ¶ 79) Advertisement owners (people who create ads for their business) place their ads on specific pages, or associate their ads with keywords in search engines, so that end users searching for relevant items may visit the ad owners' website. (*Id.* ¶ 79) ZeroAccess and similar malware skew this relation grossly. By generating non-user initiated clicks and website visits, ZeroAccess increases traffic to the ad owners' website but none of that traffic leads to potential sales. (*Id.* ¶ 79) This results in the ad owners paying the ad distributor as the ads were clicked on, but in reality the ad owner paid for traffic that was of no use. (*Id.* ¶ 79) Microsoft must constantly manage the detection and reimbursement for fraudulent clicks, which imposes cost, burden and disruption to customer relationships.

b. ZeroAccess Interferes With Advertisers Search Placement On Microsoft's Platform

Bing advertisers bid for ad placement on Bing search results. (*Id.* ¶ 80) But ZeroAccess changes the results on user's computer. (*Id.* ¶ 80) The advertiser is not charged by Bing because their link does not get clicked on, but the advertiser is harmed nonetheless: their ads are down-graded as less relevant as they are not clicked on (because ZeroAccess directs users away from the intended Bing search result). (*Id.* ¶ 80) It makes it harder for these Microsoft advertiser customers to get good placement for their ads on future search results. (*Id.* ¶ 80) It is a form of reputational harm. (*Id.* ¶ 80) There is a great risk that advertisers may attribute this problem to Microsoft and associate these problems with Microsoft's Bing and Bing Ads products, thereby diluting and tarnishing the value of these trademarks and brands. (*Id.* ¶ 81)

G. Blocking Communication Between The Infected Computers And The Fraud Control IP Addresses And Domains Is The ONLY Way To Disrupt ZeroAccess

The ZeroAccess botnet is designed to resist technical mitigation efforts, eliminating easy technical means to curb the injury being caused. (*Id.* ¶ 82) This is particularly obvious from the use of a peer-to-peer topology (with no central point of command and control that can be taken offline), the primary purpose of which is to evade actions to stop the botnet's injury and to permit the botnet to continue to grow. (*Id.* ¶ 82) Further, the Defendants have designed ZeroAccess to disable the normal security features of Windows on infected computers, and the malware files themselves are encrypted. (*Id.* ¶ 82) These actions also prevent conventional technical means to deal with the threat.

However, the activities of the botnet can be disrupted by severing communication between the ZeroAccess-infected computers and the Fraud Control IP Addresses and Fraud Control Domains listed in Appendix A, from which those infected computers get their

instructions on how to commit browser hijacking and click fraud. (*Id.* ¶ 83)

Piecemeal requests to filter traffic to Fraud Control IP Addresses and Domains, informal dispute resolution or notice to the Defendants prior to filtering the traffic would be insufficient to curb the injury. (*Id.* ¶ 84) The operators of the ZeroAccess botnet would take immediate action to defend the botnet if they were to learn of Microsoft's impending action against it. For example, they could set up computers at new IP addresses and redirect the infected computers there for instructions. (*Id.* ¶ 84)

In prior instances where security researchers or the government attempted to curb injury caused by botnets, but allowed the botnet operators to receive notice. (*Id.* ¶ 85) In these cases, the botnet operators immediately moved the botnet infrastructure to new, unidentified locations on the Internet and took other countermeasures causing the botnet to continue its operations and destroying or concealing evidence of the botnet's operations. (*Id.* ¶ 85) Indeed, when a major security service vendor attempted to neutralize ZeroAccess, the cybercriminals running ZeroAccess were quickly able to deploy a fix that largely stymied their effort to take down the botnet. (*Id.* ¶ 85)

Given the specific architecture of the ZeroAccess botnet and its use of the Fraud Control IP Addresses to communicate with and control infected user computers, if provided advance notice that those IP addresses were to be turned off, the operators of the ZeroAccess botnet would update infected computers with new (and different) IP Addresses representing new Fraud Control IP Addresses, and would destroy evidence of the botnet's operation and evidence of the infected end-user computers that need to be cleaned. (*Id.* ¶ 86)

The only way to suspend the injury caused to Microsoft, its consumers and the public, is to block the ability of the computers located at the Fraud Control IP address to communicate

instructions to the ZeroAccess-infected computers, and to redirect the associated Fraud Control Domains to secure servers. Through this relief, operational control of the ZeroAccess-infected computers will be significantly hindered, and the Internet service providers that provide services to the owners of the infected computers can notify them that they are infected and assist them in restoring their computers to normal operation and thereby liberating them from the ZeroAccess botnet. (*Id.* ¶ 82)

III. LEGAL ARGUMENT

Microsoft seeks an *ex parte* TRO and a preliminary injunction under Federal Rule of Civil Procedure 65(b), the Lanham Act, 15 U.S.C. § 1116(a), 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. As discussed below, Microsoft's requested relief is warranted here.

A. An *Ex Parte* TRO And Preliminary Injunction Blocking The Fraud Control IP Addresses Controlling The ZeroAccess Botnet Is Warranted

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. Natural Res. Def. Council, Inc.*, 555 U.S. 7, 19-23 (2008); *Dennis Melancon, Inc. v. City of New Orleans*, 703 F.3d 262, 268 (5th Cir. 2012).

Microsoft is very likely to succeed on the merits. Defendants' intrusions into protected computers, fraud, and deceptive use of Microsoft's brands violate the Computer Fraud & Abuse Act, the Electronic Communications Privacy Act and the Lanham Act. In addition, it is

deceptive, misleading and tortious conduct in violation of Texas law. Microsoft, its customers, and the public will be irreparably harmed if the ZeroAccess botnet continues to operate unabated.

By contrast, issuing the TRO and preliminary injunction Microsoft requests would not harm any legitimate interest of the Defendants. The purpose of the ZeroAccess botnet is to perpetuate illegal activity. Any effect on third-parties (ISPs, IP address hosting companies, domain registries or registrars) will be negligible and short lived. The public interest, moreover, 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, Microsoft's requested relief is warranted.

1. Microsoft Is Likely To Succeed On The Merits Of 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) violation of the Computer Fraud and Abuse Act (18 U.S.C. § 1030), (2) violation of the Electronic Communications Privacy Act (18 U.S.C. § 2701), (3) trademark infringement under the Lanham Act (15 U.S.C. § 1114), (4) false designation of origin under the Lanham Act (15 U.S.C. § 1125(a)), (5) trademark dilution under the Lanham Act (15 U.S.C. 1125(c)), (6) trespass to chattels, (7) conversion, and (8) unjust enrichment.

a. Defendants' Violate The Computer Fraud And Abuse Act

The Computer Fraud and Abuse Act ("CFAA") penalizes, *inter alia*, a party that:

- intentionally accesses a protected computer[3] without authorization, and as a result of

[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 of the United States." 18 U.S.C. § 1030(e)(2)(B).

such conduct, causes damage. 18 U.S.C. § 1030(a)(5)(C); or

- intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer. (18 U.S.C. § 1030(a)(2)(C)); or
- knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer. (18 U.S.C. § 1030(a)(5)(A)).

Microsoft's proprietary Windows operating system, the customer computers upon which it runs and Microsoft's servers in the Bing Ads advertising platform are "protected computers" under the CFAA. Defendants intentionally access Microsoft's proprietary operating system and Microsoft's customer's computers without authorization, and burden those computers by infecting them with malicious code and by executing that code without consent. Defendants intentionally access Microsoft's Bing Ads servers by introducing fraudulent Internet traffic into the servers.

ZeroAccess's intentional and unauthorized access of Microsoft's and its customers' protected computers, moreover, has resulted in substantial and damages and loss, including the costs associated with investigating the unauthorized access. Evidence submitted in support of this application demonstrates that Microsoft and their customers are damaged by this unauthorized intrusion. ZeroAccess malware's intrusion, the execution of its malicious code, and the resulting hijacking of user's computers degrades the performance of Microsoft's and its customer's computers. Microsoft must spend time and resources to combat and remediate infections of user computers caused by the ZeroAccess botnet.

ZeroAccess's unauthorized access is precisely the type of activity that the Computer

Fraud and Abuse Act is designed to prevent. *See e.g., United States v. Phillips,* 477 F.3d 215, 219 (5th Cir. 2007) (noting that CFAA is concerned with "outside hackers who break into a computer") (citations to legislative history omitted); *see also Physicians Interactive v. Lathian Sys., Inc.*, 1:03-cv-01193, 2003 U.S. Dist. LEXIS 22868, at *26 (E.D. Va. Dec. 5, 2003) (granting TRO and preliminary injunction under CFAA where defendant hacked into a computer and stole confidential information) partially abrogated on other grounds as stated in *ForceX, Inc. v. Tech. Fusion, LLC*, 2011 U.S. Dist. LEXIS 69454, at * 12 (E.D. Va. June 27, 2011); *Global Policy Partners, LLC v. Yessin*, 1:09-cv-00859, 2009 U.S. Dist. LEXIS 112472, *9-13 (E.D. Va. Nov. 24, 2009) (accessing computer using credentials that did not belong to defendant actionable under the CFAA)[4].

Further, burdening Microsoft's servers supporting Bing Ads with artificial clicks and interfering with its goodwill with advertiser customers each constitute actionable injuries under the CFAA. *See, e.g., White Buffalo Ventures, LLC v. Univ. of Texas*, 420 F.3d 366, 377 (5th Cir. 2005) (noting that actual evidence of server degradation can support loss claim sufficient to establish standing under CFAA); *Southwest Airlines Co. v. Farechase, Inc.*, 318 F. Supp. 2d 435, 439 (N.D. Tex. 2004) (CFAA standing exists where plaintiff demonstrates "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") (citation omitted); *America Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 451 (E.D. Va. 1998) (defendant's unauthorized access of plaintiff's servers violated CFAA); *Hotmail*

[4] Indeed, in recent years botnet operators who disseminate code that intrudes upon user computers, collects personal information and causes injury have been indicted and convicted criminally under the Computer Fraud & Abuse Act. *See* Heath Decl., Exs. 12 and 13 (Indictment of Jeanson James Ancheta), 15 (Sentencing of Jeanson James Ancheta).

Corp. v. Van$ Money Pie Inc., 47 U.S.P.Q.2d 1020, 1025-26 (N.D. Cal. 1998) (same). Accordingly, Microsoft is likely to succeed on the merits of its Computer Fraud & Abuse Act claim.

b. Electronic Communications Privacy Act

The Electronic Communications Privacy Act prohibits "intentionally access[ing] without authorization a facility through which an electronic communication is 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 Windows operating system, Internet Explorer browser and Bing search engine pages made available at end user computers are facilities through which electronic communication services are provided.

The ZeroAccess malware is installed without authorization on infected end-user computers and collects personal information without authorization or consent – including a user's search engine queries and search terms and the search results returned by Microsoft's Bing search engine. Specifically, the ZeroAccess malware captures what the user types as a search query and captures text of the results returned by Bing and, based on that information, redirects the infected user's computer to websites of the Defendant's choosing. Those search queries and terms and the search engine results are stored temporarily on the user's computer, in the Internet Explorer browser and in the Bing search engine web page. Obtaining stored electronic information in this way, without authorization, is a violation of the Electronic Communications Privacy Act. *See e.g. Lopez v. Pena*, 2:12-cv-00165, 2013 U.S. Dist. LEXIS 30299, at *7 (N.D. Tex. Mar. 5, 2013) (noting that unauthorized access of stored electronic communications is actionable under the ECPA). Thus, Microsoft is likely to succeed on the merits of its Electronic Communications Privacy Act claim.

c. Defendants' Lanham Act Violations

Section 1114(l) of the Lanham Act prohibits use of a reproduction, counterfeit, copy or "colorable imitation" of a registered mark in connection with the distribution of goods and services where such use is likely to cause confusion or mistake or to deceive. The ZeroAccess botnet creates and distributes copies of Microsoft's registered, famous, and distinctive trademarks in counterfeit, manipulated versions of Microsoft's Internet Explorer-branded browser and Microsoft's Bing-branded search engine webpage, and in fraudulent websites bearing Microsoft's trademarks. These unauthorized copies of Microsoft's trademarks deceive victims, causing them confusion, and causing them to mistakenly associate Microsoft with this activity. This is a clear violation of the Lanham Act and Microsoft is likely to succeed on the merits. *See, e.g., Microsoft Corp. v. Software Wholesale Club, Inc.*, 129 F. Supp. 2d 995, 1006 (S.D. Tex. 2000) (granting summary judgment of trademark infringement where defendant used counterfeit Microsoft trademarks, which were likely to cause confusion); *Choice Hotels Int'l, Inc. v. Patel*, 6:12-cv-00023, 2013 U.S. Dist. LEXIS 55345, at *12-14 (S.D. Tex. Apr. 16, 2013) (discussing confusion standard and noting presumption of confusion where identical marks are used).

The Lanham Act also prohibits use of a trademark, any false designation of origin, false designation of fact or misleading representation of fact which:

> is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person.

15 U.S.C. § 1125(a)(1)(A).

The ZeroAccess botnet misleadingly and falsely causes the famous and distinctive

Microsoft®, Windows®, Internet Explorer®, and Bing® trademarks to be associated with malicious conduct carried out on users' computers through improper use of Microsoft's Windows operating system. Critically, end users with ZeroAccess-infected computers will have their Internet Explorer web browser sessions hijacked; will have their Bing search results intercepted and will be redirected to other search results and websites; and will experience a loss of performance resulting from ZeroAccess's intrusion. Microsoft's advertiser customers will distort the value and effectiveness of their ad campaigns placed through Bing Ads. All of 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. *Microsoft Corp.,* 129 F. Supp. 2d at 1006.

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)(1). Here, the ZeroAccess 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. MetroPCS Wireless, Inc. v. Virgin Mobile USA, L.P.*, 3:08-cv-01658, 2009 U.S. Dist. LEXIS 88527, at * 39 (N.D. Tex. Sept. 25, 2009) ("Tarnishing occurs when a trademark is linked to products of shoddy quality, or is portrayed in an unwholesome or unsavory context, with the result that the public will associate the lack of quality or lack of prestige in the defendant's goods with the plaintiff's").

d. Conversion

Conversion is defined as the wrongful exercise of dominion and control over another's property in denial of or inconsistent with his rights. *Green Int'l Inc. v. Solis*, 951 S.W.2d 384, 391 (Tex. 1997). Here, the unauthorized installation of software onto and subsequent control over Microsoft's licensed Windows operating system software, Internet Explorer software and Bing search engine web page, and computers of customers interferes with and causes injury to the value of those properties. Thus, this conduct is an illegal trespass and also constitutes conversion. *See Sw. Bell Tel. Co. v. Iverson,* 3:11-cv-02009, 2012 U.S. Dist. LEXIS 26678, at *2 (N.D. Tex. Feb. 6, 2012) (allegations of unauthorized electronic data harvesting sufficient to state claims for trespass and conversion); *see also Kremen v. Cohen*, 337 F.3d 1024, 1034 (9th Cir. 2003) (recognizing that hacking into a computer system and injuring data supports a conversion claim); *Physicians Interactive*, 2003 U.S. Dist. LEXIS 22868, at *26 (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."); *Washington v. Riley*, 846 P.2d 1365, 1371 (Wash. 1993) (affirming conviction for "computer trespass" under Washington law for defendant's "hacking activity").

e. Trespass to Chattels

Pursuant to Texas law, the tort of trespass to chattels protects against interference with one's possessory interest in personal property. *See e.g. Carpenter v. Carpenter*, 2012 Tex. App. LEXIS 5322, at *11-12 (Tex. App. 2012). An intentional, wrongful act that interferes with the property owner's use of its property for a substantial period of time constitutes a trespass. *Id.* at n. 11 (citation omitted). Unauthorized access to a computer system or network may give rise to a claim for trespass to chattels. *See, e.g., Axis Surplus Ins. Co. v. Mitsubishi Caterpillar Forklift*

America Inc., 2011 U.S. Dist. LEXIS 148243, at * 2-3 (S.D. Tex. Dec. 27, 2011) (discussing significant jury verdict in favor of plaintiff on claims arising from unauthorized access to plaintiff's computer network, including claim for trespass to chattels); *see also White Buffalo Ventures,* 420 F.3d at 377 n.1 (discussing "digital trespass" cases based on the theory that unauthorized use of a network/computer system constitutes trespass to chattels). Here, defendants' authorized intrusion into Microsoft's Bing Ads servers by directing fraudulent clicks to that service injures Microsoft's property and constitutes a trespass. *White Buffalo Ventures,* 420 F.3d at 377 n.1; *see also Sw. Bell Tel. Co. v. Iverson,* 2012 U.S. Dist. LEXIS 26678, at *2 (recommending denial of motion to dismiss, *inter alia*, trespass claims based on unauthorized data mining in plaintiff's network); *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.").

f. Unjust Enrichment

A party may recover under the unjust enrichment theory when one person has obtained a benefit from another by fraud, duress, or the taking of an undue advantage. *Heldenfels Bros. v. Corpus Christi*, 832 S.W.2d 39, 41 (Tex. 1992). Here, without authorization, the Defendants have taken the benefit of Microsoft's servers, networks, its licensed Windows operating system software, its Internet Explorer browser and Bing search engine, and the computers of Microsoft's customers. Defendants have done so by improperly infecting these computers, and causing them to send hijack user's Internet Explorer web browser sessions and Bing search engine results to engage in click-fraud. Defendants have profited from this activity, including by attempting to direct fraudulent traffic to Microsoft's Bing Ads platform. Thus, it is certainly inequitable for the Defendants to retain this benefit. Microsoft is likely to succeed on the merits.

2. Irreparable Harm Will Result Unless A TRO And Preliminary Injunction Are Issued

Continued operation of the ZeroAccess botnet irreparably harms Microsoft, its customers, and the public. No monetary remedy could repair the harm to Microsoft or its customers caused by ZeroAccess's continued click fraud and browser hijacking operations. 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 Heath Decl. Ex. 22 (*Microsoft Corp. v. Peng Yong et al.*, Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.) (*Ex Parte* TRO and preliminary injunction to dismantle botnet command and control servers); Exs. 18 and 19 (*Microsoft v. Piatti, et al.,* Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.) (same); Exs. 14 and 15 (*Microsoft Corporation v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va., Brinkema J.) (same); Exs. 16 and 17 (*Microsoft v. John Does 1-11*, Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.) (same); Exs. 20 and 21 (*Microsoft Corp. et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.) (same); Exs. 10 & 11 (*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 the case brought by Microsoft acknowledged the substantial irreparable harm botnets cause Microsoft, its customers and Internet users generally. (Heath Decl. at Exs. 14-22.)

Microsoft and the public face the same irreparable harm caused by the ZeroAccess botnet. Thus, entry of an *ex parte* TRO disabling the ZeroAccess click fraud and browser hijacking command and control servers and an Order to Show Cause why a preliminary injunction should not issue are warranted. Microsoft is irreparably injured because the problems

associated with browser hijacking, infected end-user system performance degradation, and the distortion of the Internet advertising environment ZeroAccess causes are attributed to Microsoft – specifically Microsoft's Internet Explorer, Bing, and Bing Ads services and products. 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 and cause new malware infections through browser hijacking, 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, e.g., Petro Franchise Sys., LLC v. All Am. Props., Inc.*, 607 F. Supp. 2d 781, 795 (W.D. Tex. 2009) (loss of control over good will constitutes irreparable harm). This injury is irreparable because customers generally 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 will remain under constant threat of their computers being controlled by Defendant's click fraud and browser hijacking command and control servers 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.*, 1:06-cv-00644, 2007 U.S. Dist. LEXIS 10847, at *22 (M.D.N.C. Feb. 15, 2007) (finding irreparable harm because defendant's actions "will have significant and continuous long-term effects.")

3. 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 ZeroAccess command and control servers through which the ZeroAccess 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 Fraud Control IP addresses' purpose is to carry out illegal activity. Thus, Defendants will suffer no harm through preservation of the status quo pending adjudication of the issues in dispute. *See, e.g., Pesch v. First City Bank of Dallas*, 637 F. Supp. 1539, 1543 (N.D. Tex. 1986) (balance of hardships clearly favors injunction where enjoined activity is illegal).

Similarly, there will be only negligible impact on the third-party ISPs, hosting companies, domain registries and registrars, as the requested relief is carefully tailored to only disable access to IP addresses involved with the botnet and directs these third parties to take simple steps to assist in securing the IP addresses, and preserving evidence. The steps requested of these third parties are part of their normal business operations and this same assistance has been ordered in numerous prior cases involving malicious Internet activity. The limited assistance sought from the third party ISPs, 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. Conversely, if a TRO and preliminary injunction do not issue, the ZeroAccess botnet will continue to inflict irreparable injury on Microsoft, its customers, and the public. The botnet already includes millions of compromised user computers. New users are infected each day, 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 blocking access to the ZeroAccess servers

through which Defendants control their click fraud and browser hijacking operations will not affect any legitimate rights of the Defendants. Microsoft seeks only narrowly tailored assistance from ISPs and third-party hosting companies, domains registries and registrars, aimed at stopping Defendants' use of third-party infrastructure to facilitate Defendants' illegal activities. The requested relief will have a negligible effect on any potential legitimate interests of other third-parties. However, allowing the botnet to continue to harm Microsoft and the public while this action is adjudicated poses grave danger to many legitimate interests.

4. 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 would protect 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 ZeroAccess botnet. Similarly, every company providing legitimate advertising services and paying for legitimate Internet advertisements are at risk of being victims of ZeroAccess's click-fraud. Indeed, there is specific evidence that the ZeroAccess targets malicious activity at not only Microsoft, but companies such as Google, Yahoo!, and Apple as well. Further, ZeroAccess promotes websites containing counterfeit software, including malware designed to promote fraudulent schemes that can injure consumers. There is an overwhelming public interest in preserving the status quo and halting continued click fraud and browser hijacking operations caused by the ZeroAccess botnet while Microsoft proceeds with its claims.

Several district courts have already 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 Heath Decl. Exs. 14-22 (orders to disable botnets); *see also Physicians Interactive*, 2003 U.S. Dist. LEXIS 22868, at *29 ("[t]his Court has an

obligation to enjoin any alleged computer hackers from continuing to attack and steal [plaintiff's] proprietary information."). 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.

5. 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. Brotherhood of Teamsters & Auto Truck Drivers, Lcal No. 70*, 415 U.S. 423, 438-39 (1974) ("*Ex parte* temporary restraining orders are no doubt necessary in certain circumstances...").

If notice is given prior to issuance of a TRO, it is likely that Defendants will be able to quickly move the click fraud and browser hijacking command and control servers to new IP addresses before the TRO can have any remedial effects. Thus, providing notice of the requested TRO will undoubtedly facilitate efforts of the parties controlling the botnet.

It is well-established that *ex parte* relief is appropriate under circumstances such as the instant case, where notice would render the requested relief ineffective. *See e.g. Kelly v. Thompson*, 2010 U.S. Dist. LEXIS 31800, *3 (W.D. Tex. Mar. 31, 2010) (granting *ex parte* TRO without notice where irreparable harm would result if notice were given); *In re Vuitton Et Fils*

S.A., 606 F.2d 1, 4-5 (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,* 1:10-cv-00111, 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 . . . .")[5]

In this case, there is specific evidence that the botnet operators will attempt to move the infrastructure if notice is given—as this is precisely what they did in response to an attempt by a security firm to disable ZeroAccess through purely technical means. Where there is evidence that operators of botnets will attempt to evade enforcement attempts where they have notice, by moving the command and control servers, *ex parte* relief is appropriate. Particularly instructive here are *Microsoft Corp. v. John Does 1-27, Microsoft Corp. v. Peng Yong, and Microsoft Corp. v. Piatti*, all cases in which the district court issued *ex parte* TROs to disable botnet, recognizing the risk that Defendants would move the botnet infrastructure and destroy evidence if prior notice were given. (*See* Heath Decl., Exs. 14, 15, 18, 19, and 22.)

Similarly, in *FTC v. Pricewert LLC*, the district court issued an *ex parte* TRO suspending Internet connectivity of a company enabling botnet activity and other illegal computer-related

---

[5] *See also Crosby v. Petromed, Inc.*, 2:09-cv-05055, 2009 U.S. Dist. LEXIS 73419, at *5 (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..."); *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); *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").

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* Heath Decl., Ex. 10 (*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*, 1:07-cv-22674, 2007 U.S. Dist. Lexis 98676, at *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.

B. The All Writs Act Authorizes The Court To Direct Third Parties To Perform Acts Necessary To Avoid Frustration Of The Requested Relief

Microsoft's Proposed Order directs that the third-party ISPs whose infrastructure Defendants rely on to operate the botnet reasonably cooperate to effectuate the order. Critically, these third-parties are the only entities that can effectively disable Defendants' click fraud and browser hijacking command and control infrastructure, and thus their cooperation is necessary.[6]

The All Writs Act provides that a court may issue all writs necessary or appropriate for the administration of justice. 28 U.S.C. § 1651(a). The Supreme Court has recognized that narrow direction to third-parties necessary to effect the implementation of a court order is authorized by the All Writs Act:

> The power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice, and encompasses even those who have not taken any affirmative action to hinder justice.

[6] The Proposed Order also includes a non-binding request for voluntarily cooperation from hosting companies through which Defendants procured the IP addresses and domains used to control click fraud and browser hijacking operations.

United States v. New York Tel. Co., 434 U.S. at 174 (citations omitted) (order to telephone company to assist in implementation of a pen register warrant was authorized under the All Writs Act); *Moore v. Tangipahoa Parish Sch. Bd.*, 507 Fed. App'x. 389, 396 (5th Cir. 2013) (unpublished) ("The All Writs Act provides 'power to a federal court to issue such commands . . . as may be necessary or appropriate to effectuate and prevent the frustration of orders it has previously issued in its exercise of jurisdiction otherwise obtained.'") (citing *New York Tel. Co.*, 434 U.S. at 172); *see also In re Application of United States for an Order Authorizing An In-Progress Trace of Wire Commc'ns Over Tel. Facilities*, 616 F.2d 1122, 1129 (9th Cir. 1980) (same; noting of *New York Tel. Co.*, "the Court made the commonsense observation that, without the participation of the telephone company, 'there is no conceivable way in which the surveillance authorized could have been successfully accomplished.'" 434 U.S. at 172); *In re Baldwin-United Corp.*, 770 F.2d 328, 338-339 (2d Cir. 1985) ("An important feature of the All-Writs Act is its grant of authority to enjoin and bind non-parties to an action when needed to preserve the court's ability to reach or enforce its decision in a case over which it has proper jurisdiction"; "We do not believe that Rule 65 was intended to impose such a limit on the court's authority provided by the All-Writs Act to protect its ability to render a binding judgment."); *Dell Inc.*, 2007 U.S. Dist. LEXIS 98676, at *16 (All Writs Act applied in conjunction with trademark seizure under Rule 65 and Lanham Act).

Requiring these third parties to reasonably assist in the execution of this order will not offend due process as the Proposed Order requires (1) only minimal assistance from the third parties in executing the order (acts that they would take in the ordinary course of their operations), (2) that it be implemented with the least degree of interference with the normal operation of third parties, (3) does not deprive the third parties of any tangible or significant

property interests and (4) requires Microsoft to compensate the third-parties for the assistance rendered. If, in the implementation of the Proposed Order, any third-party wishes to bring an issue to the attention of the Court, Microsoft will bring it immediately. The third-parties will have an opportunity to be heard at the preliminary injunction hearing, which must occur shortly after the execution of the Proposed Order. Fed. R. Civ. P. 65(b)(2). The directions to third-parties in the Proposed Order are thus narrow, satisfy Due Process, and are necessary to effect the requested relief and ensure that the relief is not rendered fruitless. Moreover, Microsoft has already notified ISPs of this action, is working cooperatively with them and has received their input on the terms of the proposed order submitted with this motion.

C. 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 Defendants and to serve the complaint.

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. (*Id.* ¶¶ 7-9, Ex. 1.) 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 ZeroAccess IP addresses. (*Id.* ¶ 10.) When Defendants registered the IP addresses, 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. (*Id.* ¶¶ 30-34.)

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. (*Id.* ¶ 11.)

Microsoft Will Provide Notice To Defendants By Personal Delivery: Microsoft has identified IP addresses from which the ZeroAccess 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. Moreover, it is anticipated that Microsoft's effort to obtain contact information for Defendants will be facilitated by the request for voluntary cooperation from hosting companies included in the Proposed Order. 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 any valid addresses that are identified in the U.S. (Heath Decl. ¶ 13.)

Microsoft Will Provide Notice By Personal Delivery And Treaty If Possible: If valid physical addresses of Defendants can be identified, Microsoft will notify Defendants and serve process upon them by personal delivery or through the Hague Convention on service of process or similar treaty-based means. (*Id.* ¶ 14.)

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. Here, Defendants are believed to reside in the Russian Federation, which has currently suspended the Hague Convention, thus the appropriate analysis of service is under Fed. Rule Civ. P. and the underlying principles of Due Process.[7]

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., Keller Williams Realty, Inc. v. Lapeer,* 4:08-cv-01292, 2008 U.S. Dist. LEXIS 58079, at *5 (S.D. Tex. July 31, 2008) (citing *Rio Props., Inc. v. Rio Int'l. Interlink*, 284 F.3d 1007, 1017 (9th Cir. 2002) (authorizing service by e-mail upon an international defendant); Heath 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*, 1:01-cv-10132, 1:01-cv-10144, 2001 U.S. Dist. LEXIS 21712 (S.D.N.Y. Dec. 26, 2001) (authorizing service by publication upon Osama bin Laden and the al-Qaeda

---

[7] *See* http://travel.state.gov/law/judicial/judicial_3831.html (State Department observing that Hague Convention has been suspended by Russian Federation); *RSM Prod. Corp. v. Fridman*, 2007 U.S. Dist. LEXIS 58194, *5-6 (S.D.N.Y. 2007) (approving service of process by non-treaty based means upon an individual defendant in Russia, in view of suspension of Hague Convention processes); *Xcentric Ventures, LLC v. Karsen, Ltd.*, 2011 U.S. Dist. LEXIS 81698 (D. Ariz. 2011) (same; permitting service of process upon defendant in Russia by email under Rule 4(f)(3), in light of suspension of Hague Convention processes); *Henry F. Teichmann, Inc. v. Caspian Flat Glass OJSC*, 2013 U.S. Dist. LEXIS 54299, *3 (W.D. Pa. 2013) (Regarding defendant in Russia: "[b]ecause it would be futile, Plaintiff need not first attempt service through the Hague Service Convention."); *Arista Records LLC v. Media Servs. LLC*, 2008 U.S. Dist. LEXIS 16485 (S.D.N.Y. 2008) (plaintiff need not first attempt service on Russian Defendant in accordance with the Hague Convention for service pursuant to Rule 4(f)(3) to be proper).

organization); *FMAC Loan Receivables v. Dagra*, 228 F.R.D. 531, 535-36 (E.D. Va. 2005) (acknowledging that courts have readily used Rule 4(f)(3) to authorize international service through non-traditional means); *BP Prods. 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, at *3 (D. Md. Jan. 20, 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 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 ebusiness scofflaw, playing hide-and-seek with the federal court, e-mail may be the only means of effecting service of process.

Rio Props., Inc., 284 F.3d at 1018; *see also Williams-Sonoma, Inc. v. Friendfinder*, Inc., 3:06-cv-06572, 2007 U.S. Dist. LEXIS 31299, at *5-6 (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 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, 315-16 (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[8].

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 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.

IV. CONCLUSION

For the reasons set forth herein, Microsoft respectfully requests that this Honorable Court grant its application 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.

[8] 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 Prods. N. 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.")

Dated: November 25, 2013

Respectfully submitted

FISH & RICHARDSON P.C.

By: _____

David M. Hoffman
Texas Bar No. 24046084
hoffman@fr.com

William Thomas Jacks
Texas Bar No. 10452000
jacks@fr.com

111 Congress Ave, Suite 810
Austin, TX 78701
Telephone: +1 (512) 472-5070
Facsimile: +1 (512) 320-8935

Of Counsel:

ORRICK, HERRINGTON & SUTCLIFFE LLP

Gabriel M. Ramsey
(*pro hac vice application pending*)
gramsey@orrick.com

Jeffrey L. Cox
(*pro hac vice application pending*)
jcox@orrick.com

Jacob M. Heath
(*pro hac vice application pending*)
jheath@orrick.com

Robert L. Uriarte
(*pro hac vice application pending*)
ruriarte@orrick.com

1000 Marsh Road
Menlo Park, California 94025
Telephone: +1 (650) 614-7400
Facsimile: +1 (650) 614-7401

Counsel for Plaintiff
MICROSOFT CORPORATION