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

COMPLAINT

Plaintiff MICROSOFT CORP. ("Microsoft") hereby complains and alleges against JOHN DOES 1-8 ("Doe Defendants") (referred to collectively herein as "Defendants"), controlling the "ZeroAccess" botnet using the Internet Protocol (IP) addresses and Internet domains set forth at Appendix A this Complaint ("the ZeroAccess Fraud Control IP Addresses and Fraud Control Domains"), as follows:

NATURE OF ACTION

1. This is an action based upon: (1) The Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) Electronic Communications Privacy Act, 18 U.S.C. § 2701; (3) Trademark Infringement under the Lanham Act, 15 U.S.C. § 1114 *et seq.* (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) Common Law Trespass to Chattels; (7) Unjust Enrichment; and (8) Conversion. Microsoft seeks injunctive and other equitable relief and damages against the operators of a controlled network of computers, known as the "ZeroAccess" botnet, by means of the ZeroAccess Fraud Control IP Addresses and Fraud Control Domains that have and continue

to cause irreparable injury to Microsoft, its customers, and the public.

PARTIES

2. Plaintiff Microsoft is a corporation duly organized and existing under the laws of the State of Washington, having its headquarters and principal place of business in Redmond, Washington.

3. John Doe 1 controls the ZeroAccess Fraud Control IP addresses 188.40.114.195 and 188.40.114.228 and Fraud Control Domains qvhobsbzhzhdhenvzbs.com, mbbcmyjwgypdcujuuvrlt.com, wuyigrpdappakoahb9.com, jzlevndwetzyfryruytkzkb.com, glzhbnbxqtjoasaeyftwdmhzjd.com, kttvkzpwufmrditdojlgytxyb.com, vgfsowmleomwconnxmnyfhle.com, and vmtsukcbbqmmndojqirbbij.com set forth in Appendix A that are being misused to cause harm to Microsoft, its customers, and the public. Microsoft is informed and believes and thereupon alleges that John Doe 1 can likely be contacted directly or through third-parties using the following information: 15528566292361-b434c0@whoisprivacyservices.com.au, b894a578787a6d5767d4f3cad9e25b63-1429447@contact.gandi.net, privacy@dynadot.com, Hetzner Online AG ("Hetzner"), at Datacenter 10, Stuttgarter Strasse 1, D-9710 Gunzenhausen, Germany, abuse@hetzner.de. ZeroAccess Fraud Control IP addresses 188.40.114.195 and 188.40.114.228 are designated as IP addresses maintained by Hetzner.

4. John Doe 2 controls the ZeroAccess Fraud Control IP addresses 83.133.120.185 and 83.133.120.187 and Fraud Control Domains gozapinmagbclxbwin.com, nbqkgysciuuhadgpjfquvpu.com, cjelaglawfoyidgyapv.com, jpciukjdkqxgreoikpgya.com, qhdsxosxtvmhurwezsipzq.com, omakfdwkhrpqudxvapy.com, chvhcncpqttfpcibtmetg.com, ezcfogjitbqwnornezx.com, rwdtklvrqnffdqkyuugfklip.com, uinrpbrfrnqggtorjdpqg.com, xlotxdxtorwfmvuzfuvtspel.com, mkvrpknidkurcrftiqsfjqdxbn.com, waajenyndxxbjolsbesd.com, jgisypzilnrperlwcionbt.com, and fwmavqvphidhnrxcxvcnx.com set forth in Appendix A that are being misused to cause harm to Microsoft, its customers, and the public. Microsoft is informed and believes and thereupon alleges that John Doe 2 can likely be contacted directly or through

third-parties using the following information: admin@overseedomainmanagement.com, 1af43616f137467387028c41f73e7f0a.protect@whoisguard.com, jgou.veia@gmail.com, xlotxdxtorwfmvuzfuvtspel.com@domainsbyproxy.com, mkvrpknidkurcrftiqsfjqdxbn.com@domainsbyproxy.com, b894a578787a6d5767d4f3cad9e25b63-1429447@contact.gandi.net; privacy@dynadot.com; Greatnet New Media ("Greatnet") at Brentenstrasse 4a, D-83734 Hasusham, Germany; at Stromstrabe 11-5, 10555 Berlin, Germany; abuse@greatnet.de. ZeroAccess Fraud Control IP addresses 83.133.120.185 and 83.133.120.187 are designated as IP addresses maintained by Greatnet.

5. John Doe 3 controls the ZeroAccess Fraud Control IP address 195.3.145.108 and Fraud Control Domains dclixvfpttrlcnindvrnyeic.com, evtrdtikvzwpscvrxpr.com, atenrqqtfrzozqrqbdzwkxzyuc.com, and oqcllyhefbhhaijaxq.com set forth in Appendix A that is being misused to cause harm to Microsoft, its customers, and the public. Microsoft is informed and believes and thereupon alleges that John Doe 3 can likely be contacted directly or through third-parties using the following information: bdd243a7cae540e08484e24e71552520.protect@whoisguard.com, b894a578787a6d5767d4f3cad9e25b63-1429447@contact.gandi.net; RN Data SIA ("RN Data") at Maskavas 322, LV-1063, Riga, Latvia; admin@altnet.lv. ZeroAccess Fraud Control IP address 195.3.145.108 is designated as an IP address maintained by RN Data.

6. John Doe 4 controls the ZeroAccess Fraud Control IP address 178.239.55.170 set and Fraud Control Domains jgvkfxhkhbbjoxggsve.com and litcyleyzrglkulaifkrx.com forth in Appendix A that are being misused to cause harm to Microsoft, its customers, and the public. Microsoft is informed and believes and thereupon alleges that John Doe 4 can likely be contacted directly or through third-parties using the following information: Netrouting Ellada Projects BV ("Netrouting") at Boylewg 2, 3208 KA, Spikenisse, the Netherlands; abuse@netrouting.com; privacy@dynadot.com. ZeroAccess Fraud Control IP address 178.239.55.170 is designated as an IP address maintained by RN Data.

7. John Doe 5 controls the ZeroAccess Fraud Control IP addresses 217.23.3.225, 217.23.3.242, and 217.23.9.247 and Fraud Control Domains hzhrjmeeczcgxodmqyz.com, fnyxzjeqxzdpeocarhljdmyjk.com, sqdfmslznztfozshtidmigmsbh.com, vdlhxlmqhfafeovqohwrbaskrh.com, nmfvaofnginwocnidecxnpcs.com, euuqddlxgrnxlrjjbhytukpz.com, vzsjfnjwchfqrvylhdhxa.com, vjlvchretllifcsgynuq.com, dxgplrlsljdjhqzqajkcau.com, qbsiauhmoxfkrgfqey.com, ssarknpzvpkteqnaia.com, and adhavzpbykyffaxqtts.com set forth in Appendix A that are being misused to cause harm to Microsoft, its customers, and the public. Microsoft is informed and believes and thereupon alleges that John Doe 5 can likely be contacted directly or through third-parties using the following information: 16520144097161-049ee1@whoisprivacyservices.com.au, 433f8f3c35244b459c599e0b004701c4.protect@whoisguard.com, vjlvchretllifcsgynuq.com@domainsbyproxy.com, jgou.veia@gmail.com, privacy@dynadot.com, b894a578787a6d5767d4f3cad9e25b63-1429447@contact.gandi.net, a8bd2de2c86841008163bb70ec85185e.protect@whoisguard.com, 7fe1e2f261e848abb774e42e6ffa1615.protect@whoisguard.com; WorldStream at Industriestaat 24, 2671CT Naaldwijk, the Netherlands; abuse@worldstream.nl. ZeroAccess Fraud Control IP addresses 217.23.3.225, 217.23.3.242, and 217.23.9.247 are designated as IP addresses maintained by Worldstream.

8. John Doe 6 controls the ZeroAccess Fraud Control IP addresses 46.249.59.47 and 46.249.59.48 and Fraud Control Domains loanxohaktcocrovagkaa.com, mxyawkwuwxdhuaidissclggy.com, erspiwscuqslhjflgbbgcfbc.com, spujplpdupiwbghiedhqeja.com, xttfdqrsvlkvmtewgiqolttqi.com, jlcemszzlsfvtvwsszrysooca.com, eagdbqufytdxvzbavzriwzgw.com, and spujplpdupiwbghiedhqeja.com set forth in Appendix A that are being misused to cause harm to Microsoft, its customers, and the public. Microsoft is informed and believes and thereupon alleges that John Doe 6 can likely be contacted directly or through third-parties using the following information: Serverius Holding B.V ("Serverius") at De Linge 26, 8253 PJ, Dronten, the Netherlands; abuse@serverius.nl,

b894a578787a6d5767d4f3cad9e25b63-1429447@contact.gandi.net, privacy@dynadot.com. ZeroAccess Fraud Control IP addresses 46.249.59.47 and 46.249.59.48 are designated as IP addresses maintained by Serverius. Microsoft is informed and believes and thereupon alleges that John Doe 6 also can likely be contacted through third party Maikel Uerlings at email address: cust597@serverius.com.

9. John Doe 7 controls the ZeroAccess Fraud Control IP addresses 46.19.137.19, 81.17.18.18, and 81.17.26.189 set forth in Appendix A that are being misused to cause harm to Microsoft, its customers, and the public. Microsoft is informed and believes and thereupon alleges that John Doe 7 can likely be contacted directly or through third-parties using the following information: Private Layer Inc. ("Private Layer") at Zurcherstrasse 161, SPB 101280, 8010 Zurich, Switzerland; at SwissPost 9865, Zurcherstrasse 161, 8010 Zurich, Switzerland; abuse@privatelayer.com; Hossein Abili Nejad at Hasen Tape st1, Baku, az2156, Azerbaijan; hamihost@gmail.com. ZeroAccess Fraud Control IP addresses 46.19.137.19, 81.17.18.18, and 81.17.26.189 are designated as IP addresses maintained by Private Layer.

10. John Doe 8 controls the ZeroAccess Fraud Control IP addresses 94.242.195.162, 94.242.195.163, and 94.242.195.164 set forth in Appendix A that are being misused to cause harm to Microsoft, its customers, and the public. Microsoft is informed and believes and thereupon alleges that John Doe 8 can likely be contacted directly or through third-parties using the following information: Root SA ("Root") at 3, op der Poukewiss, 7795 Roost-Bissen, Luxembourg; abuse@as5577.net. ZeroAccess Fraud Control IP addresses 94.242.195.162, 94.242.195.163, and 94.242.195.164 are designated as IP addresses maintained by Root.

11. Third parties VeriSign Naming Services and VeriSign Global Registry Services (collectively "VeriSign") are the domain name registry that oversees the registration of all domain names ending in ".com," including all of the ZeroAccess ".com" Fraud Control Domains. Verisign Name Services is located at 21345 Ridgetop Circle, 4th Floor, Dulles, Virginia 20166. Verisign Global Registry Services is located at 12061 Bluemont Way, Reston, Virginia, 20190.

12. Defendants own, operate, control, and maintain the ZeroAccess botnet and do business under the names of the ZeroAccess Fraud Control IP Addresses and Fraud Control Domains.

13. Microsoft will amend this complaint to allege the Doe Defendants' true names and capacities when ascertained. Microsoft will exercise due diligence to determine Doe Defendants' true names, capacities and contact information, and to effect service upon those Doe Defendants.

14. Microsoft is informed and believes and therefore alleges that each of the fictitiously named Doe Defendants is responsible in some manner for the occurrences herein alleged, and that Microsoft's injuries as herein alleged were proximately caused by such Doe Defendants.

15. Doe Defendants have provided the contact information for the Bamital domains and IP addresses set forth at Appendix A to this Complaint.

16. The actions and omissions alleged herein to have been undertaken by the Defendants were undertaken by each Defendant individually, were actions and omissions that each Defendant authorized, controlled, directed, or had the ability to authorize, control or direct, and/or were actions and omissions each Defendant assisted, participated in, or otherwise encouraged, and are actions for which each Defendant is liable. Each Defendant aided and abetted the actions of the Defendants set forth below, in that each Defendant had knowledge of those actions and omissions, provided assistance and benefited from those actions and omissions, in whole or in part. Each of the Defendants was the agent of each of the remaining Defendants, and in doing the things hereinafter alleged, was acting within the course and scope of such agency and with the permission and consent of other Defendants.

JURISDICTION AND VENUE

17. This action arises out of Defendants' violation of the Federal Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701) and the Lanham Act (15 U.S.C. §§ 1114 & 1125). Therefore, the Court has subject matter

jurisdiction of this action based on 28 U.S.C. § 1331. This is also an action for trespass to chattels, unjust enrichment, conversion and negligence. Accordingly, this Court has subject matter jurisdiction under 28 U.S.C. § 1367.

18. Upon information and belief, Defendants maintain computers and Internet websites and engage in other conduct availing themselves of the privilege of conducting business in, have directed acts complained of herein toward and have utilized instrumentalities located in Texas and the Western District of Texas to carry out the acts complained of herein.

19. Defendants have affirmatively directed actions at Texas and the Western District of Texas by directing malicious computer code at the computers of individual users located in Texas and the Western District of Texas, attempting to infect those user computers with the malicious code and to make the user computers part of the "botnet," which is used to injure Microsoft, its customers and the public. The following **Figure 1** depicts the geographical location of user computers in Texas and the Western District of Texas against which Defendants are known to have directed malicious code, attempting to infect those computers and enlist them in the botnet:

Fig. 1

Texas **Austin**

20. Defendants have undertaken the acts alleged herein with knowledge that such acts

would cause harm by directing malicious code to user computers located in the Western District of Texas, thereby injuring Microsoft, its customers, and others both in the Western District of Texas and elsewhere in the United States. Therefore, this Court has personal jurisdiction over Defendants.

21. Pursuant to 28 U.S.C. § 1391(b), venue is proper in this judicial district. A substantial part of the events or omissions giving rise to Microsoft's claims, together with a substantial part of the property that is the subject of Microsoft's claims, are situated in this judicial district. Venue is proper in this judicial district under 28 U.S.C. § 1391(c) because the Defendants are subject to personal jurisdiction in this judicial district.

FACTUAL BACKGROUND

Microsoft's Software, Services and Reputation

22. Microsoft® is a provider of the Windows® operating system, the Internet Explorer® web browser, the Bing® search engine, and the Bing® Ads advertising platform, and a variety of other software and services. Microsoft has invested substantial resources in developing high-quality products and services. 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, establishing a strong brand and developing 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 Microsoft®, Windows®, Internet Explorer®, and Bing® marks. Copies of the trademark registration numbers 2872708, 2463526, 2277112, and 3883548 for the Microsoft, Windows, Internet Explorer and Bing trademarks are attached at Appendix C to this Complaint.

Internet Advertising And Click-Fraud

23. Online advertising is a multibillion dollar a year industry with U.S. online advertising expenditures reaching $20.1 billion in the first half of 2013, and growing at 18% per

year. Its size and rapid growth combined with its highly technical and organizational complexity has made online advertising a rich environment for cybercriminals who have devised multiple schemes to manipulate the online advertising business model, siphoning many millions of dollars annually. Cybercriminals have developed methods of gaining control over user computers, typically by infecting the computers with malicious software, known as "malware."

24. Microsoft contracts with companies who wish to place advertisements on the Internet. Through Microsoft's Bing Ads platform advertisers manage their online campaigns, using the results of their past ad campaigns to dictate future online campaigns. Microsoft places advertisements on, among other places, a network of websites of third-parties – called "publishers" – that also participate in Microsoft's advertising network program. Google, Yahoo! and others also provide large-scale advertising platforms similar to Bing Ads.

25. A user viewing a publisher's website can click on an advertisement that will connect the individual to the advertiser's website where additional information about the product or service being advertised will be displayed. The advertiser's goal is to encourage the end user to take additional actions – *e.g.*, requesting more information or purchasing products or services. These additional actions taken on an advertiser's website can be tracked and monitored by advertisers.

26. In a "pay-per-click" advertising model, when a consumer clicks on an advertisement, the advertising platform charges the advertiser and pays the publisher of the website where the click occurred. Advertisers, however, are generally not charged for clicks of dubious quality or origin or that appear illegitimate. Pay-per-click systems allow publishers to profit from the time, effort, and money invested in developing interesting and useful websites without requiring them to directly charge users for access to their websites. Advertisers benefit by placement of advertisements on websites likely to attract end-users interested in their products or services. In pay-per-click models, advertisers benefit by being connected directly with individuals who have, by clicking on an advertisement, shown an interest in their products or services.

27. Pay-per-click systems, however, are not immune to fraud. Unscrupulous publishers could, for example, use automated scripts, end-user computers infected with malware, or hired-individuals to generate a large number of clicks on the advertisements placed on their own websites by Bing Ads or other advertising platforms. These methods merely imitate a legitimate user's clicking of an advertisement for the sole purpose of generating a charge per click, but fail to reflect or monetize any interest in the product or service being advertised. Those clicks are considered fraudulent and the activity is termed "click-fraud." A publisher engaged in click-fraud can reap ill-gotten profits because, for each click recorded, the publisher is paid at the expense of the advertiser whose advertisement was clicked.

28. There are more sophisticated schemes where cybercriminals can generate large quantities of invalid clicks by redirecting innocent end-users' web browsers to websites, deceiving the end-users into clicking on online advertisements. Techniques to channel users to particular websites may include installing malware on end-users' computers that cause users to visit the sites or purchasing Internet traffic from parties that control such malware. Collections of such computers infected with this type of malware, called botnets, can generate a massive number of fraudulent clicks on advertisements or websites, without the knowledge or consent of the victims, internet advertising platforms and technology providers such as Microsoft. Botnets that are specialized for this purpose are referred to as "click-bots."

29. The "bad traffic" generated from such botnets is bought and sold in a complex ecosystem of brokers and traffic trading. Parties that purchase bad traffic, knowingly or unknowingly, can ultimately profit from it by using it to drive up the number of clicks on the advertisements placed on websites. Advertisers who have paid to have online advertisements placed on the Internet expecting that they will be promoted by legitimate means, may ultimately pay for invalid clicks generated through these schemes.

30. End users are also harmed by click-fraud. Their computers may be enlisted in illegal schemes, their browser searches hijacked, and the performance of their computers degraded. Once a user's computer is infected with malware that gives a cybercriminal control

over the computer for one purpose, the computer becomes an asset that the cybercriminal can sell or rent to other cybercriminals for additional illegal activities, many aimed directly at spying on or stealing from the unsuspecting owner of the infected computer. Click-fraud and the money that it creates for cybercriminal operations has a far wider impact than the advertising industry itself, and it places at risk all those who use the Internet.

Computer "Botnets"

31. A "botnet" is a collection of individual computers, each running software that allows communication among those computers and allows centralized or decentralized communication with other computers providing control instructions. The individual computers in a botnet often belong to individual users who have unknowingly downloaded or been infected by malware, assimilating computer into botnet. A user's computer, for example, may become part of a botnet when the user inadvertently interacts with a malicious website advertisement, clicks on a malicious email attachment, or downloads malware. In each such instance, software code is downloaded or executed on the user's computer, causing that computer to become part of the botnet. Once part of the botnet, the user's computer is capable of sending and receiving communications, code and instructions to or from other botnet computers.

32. Some botnet computers are wholly within the control of the botnet creator. These may have specialized functions, such as sending control instructions. These may be referred to as "command and control" computers.

33. Botnets are often created and controlled by sophisticated criminal organizations and are used to carry out misconduct that harms others' rights. Cybercriminals, for example, may use a computer in a botnet to anonymously send unsolicited, bulk email without the knowledge or consent of the individual user who owns the compromised computer. Similarly, they may also use a computer to deliver further malware to infect other computers, making them part of the botnet as well. Cybercriminals may also be used an infected computer to carry out fraud, computer intrusions or other misconduct. A botnet computer may also be used simply to "proxy" or relay Internet communications originating from other computers, to obscure and to

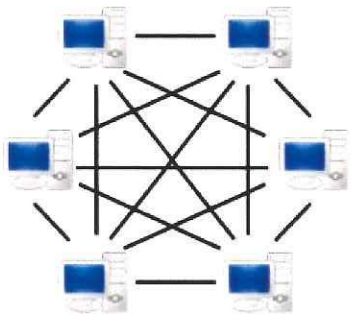
conceal the true source of those communications.

The ZeroAccess Botnet: Overall Architecture

34. Microsoft brings this action to stop Defendants from harming Microsoft and its customers through the malicious use of domains and IP addresses that are central to a botnet known as the "ZeroAccess" botnet – also known as "Sirefef" or "max++".

35. The ZeroAccess botnet has a Peer-to-Peer topology that can be represented as follows:

Peer-To-Peer Network



36. This architecture is employed as a way to resist countermeasures. 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. In other words, in a peer-to-peer network, any one of the infected computers can function as a command-and-control server. Consequently, there is no single point of command and control that provides an easy target for those seeking to disrupt the entire network. Because a peer-to-peer botnet is the most difficult type of botnet topology to disrupt, peer-to-peer topologies are especially attractive to cybercriminals designing and propagating botnets. Peer-to-peer topologies are also advantageous for cybercriminals because their architecture allows for more robust communications between the compromised computers, making the botnet as a whole more resilient against efforts to disrupt the botnet. Due to its network architecture, ZeroAccess is one of the most robust and durable botnets on the Internet today.

37. When unsuspecting users browse one of these websites, the user's computers is taken to another website where malware called an "exploit pack" is downloaded and silently probes the computer for vulnerabilities, looking for an opportunity to execute code or place the malware onto the system. Once installed, the exploit pack downloads and installs the ZeroAccess malware.

38. Once infected, Defendants direct ZeroAccess-infected computers to engage in click-fraud either through hijacking the web browsers of the ZeroAccess-infected computers or by instructing the infected computers to generate automated Internet traffic. ZeroAccess' modular structure allows Defendants to use ZeroAccess-infected computers to perform other illegal activity, including personal identity theft and "DDOS" attacks that render entire computer networks inoperable. Most if not all owners of ZeroAccess-infected computers are unaware that their machines are infected and operating as part of the ZeroAccess botnet.

The ZeroAccess Fraud Control IP Addresses And Fraud Control Domains

39. The ZeroAccess botnet uses IP addresses and Internet domains to control the ZeroAccess-infected computers to communicate with each other and to expand the botnet. These IP addresses and domains are discrete and relatively static.

40. The infected computers in the peer-to-peer network rely on this separate set of servers located at 18 IP addresses and 49 Internet domains maintained by Defendants at hosting companies in Latvia, Luxembourg, Switzerland, the Netherlands, and Germany. When ZeroAccess first infects a computer, the newly-infected computer does not contain the files or modules required to commit actual click fraud or browser hijacking. Rather, the newly-infected computer must acquire the files and modules from the first peer it contacts. Each time a ZeroAccess-infected computer contacts any other peer, it also asks what other ZeroAccess modules or files that peer possesses. The files that the ZeroAccess-infected computer will acquire in this fashion contains a list of IP addresses representing servers that are not part of the peer-to-peer network, but instead provide the infected computer explicit instructions on how to commit the click fraud or browser hijacking. The list of IP addresses changes gradually over

time. Currently there are 18 IP addresses (the "Fraud Control IP Addresses"). Microsoft is informed and believes and thereupon alleges that the ZeroAccess botnet operators use the 49 Internet domains (the "Fraud Control Domains") as a fall-back mechanism to support and to maintain the ZeroAccess botnet should the botnet come under attack. The Fraud Control Domains are listed in Appendix A to the Complaint.

41. The Fraud Control IP Addresses send infected computers information and instructions over the Internet that forces those computers to engage in "browser hijacking." Browser hijacking occurs when the ZeroAccess malware takes control of an infected computer's web browser and redirects the user to a search website of the botnet operator's choosing. ZeroAccess specifically targets searches on Microsoft's Bing search engine as well as Google and Yahoo!. A user, for example, may use Microsoft's Internet Explorer web browser and Microsoft's Bing search engine to search for products, services or issues of interest. Bing will return a list of results that the user will review and eventually click on. As soon as the user clicks on one of the links, the ZeroAccess malware running on the user's computer redirects the user's Internet Explorer browser and Bing search results and redirects Internet Explorer and the Bing search results to a Fraud Control IP Address and then redirects the user to one of several possible websites predetermined by Defendants. In so doing, the ZeroAccess malware is misrepresenting to the user that they are using the Bing-branded search engine containing Microsoft's Bing trademark and the Internet Explorer-branded browser. In reality, the server at the Fraud Control IP Address redirects the user's Internet Explorer browser and Bing search to websites predetermined by the botnet operators.

42. The Fraud Control IP Addresses also send infected computers information and instructions over the Internet that forces those computers to engage in "click-fraud." Click-fraud occurs when the ZeroAccess malware forces an infected computer to generate automated Internet traffic by instructing those computers – without the user's knowledge or intervention – to connect to any website that Defendants choose. When ZeroAccess-infected computers are turned on, the ZeroAccess malware running on those computers will connect with one or more of

the Fraud Control IP Addresses listed in Appendix A. The computers at those IP addresses and domains provide the ZeroAccess-infected computer with a list of URLs, each pointing to a website to connect. The ZeroAccess malware then launches a "hidden" instance of a web browser – such as Microsoft's Internet Explorer – on the infected computers and causes the hidden browser to visit those websites that Defendants as though it were a real user. When a ZeroAccess-infected computer connects to a website that contains an advertisement, the browser on the infected computer downloads the advertisement. At that point, the ZeroAccess malware stimulates a click on the advertisement. In then moves on to the next website in this list and repeats the process. The owner of the infected computer – even if they were sitting at the computer – would not see the hidden browser. The owner, however, would experience a loss in performance of both the computer and the Internet connection, given the substantial amount of Internet connections the ZeroAccess malware forces the infected computer to perform.

43. By instructing ZeroAccess-infected computers to connect to the Fraud Control IP Addresses set forth in Appendix A and then having those infected computers receive instructions from the Fraud Control IP Addresses in order to engage in browser hijacking and click-fraud, Defendants use each of the Fraud Control IP Addresses to support and to propagate the ZeroAccess botnet and further its malicious activity. Upon information and belief, Defendants, moreover, use the Fraud Control Domains as a fallback mechanism to support and maintain the ZeroAccess botnet.

Injury Caused By The ZeroAccess Botnet To Microsoft And Its Customers

44. The ZeroAccess malware is clandestinely introduced onto users' computers, infecting those computers and making them part of the botnet. These acts constitute an unauthorized intrusion into the Microsoft Windows® operating system which Microsoft licenses to the end users. ZeroAccess, for example, writes particular entries to the registry of Windows® operating system, without the consent of Microsoft or its customers, including commands that tell the computer which commands to execute, commands that facilitate communication between botnet computers, commands which force the computer to engage in click-fraud, commands that

tell the computer how to receive instructions from the botnet operator and data identifying the computer within the botnet. The registry is a primary repository of crucial information the computer needs to run correctly.

45. ZeroAccess creates hidden directories, overwrites software drivers needed by the operating system and injects itself into low-level processes. ZeroAccess disables security features on infected computers, lowering security credentials and disabling Windows security, leaving the computer susceptible to secondary infections. It disables Base FilteringEngine Service, IP Helper service, Windows firewall service, Windows Defender service, Windows Security Center Service, and Proxy Auto Discovery Service. ZeroAccess, by disabling these services, keeps infected computers from, among other things, retrieving security updates from Microsoft. These events take place without the knowledge or authorization of the user, as ZeroAccess runs as a background process invisible to the user without any user-interface, giving the computer's owner no indication that ZeroAccess is present or running.

46. The ZeroAccess botnet's intrusion into Microsoft's Windows® operating system is without the authority of Microsoft or its customers and exceeds any authority granted by Microsoft or its customers to any third party, including the operators of the ZeroAccess botnet.

47. The ZeroAccess botnet harms Microsoft's customers by misusing the Windows® operating system on those users' infected computers. The ZeroAccess botnet causes harm to Microsoft's customers by, among other things, causing customers' computers to:

a. install and run software without the customers' knowledge or consent, including software to support the botnet infrastructure, software that causes the computer to engage in click-fraud through browser hijacking and through the generation of automated Internet traffic, and software enabling the computer to engage in other unauthorized activities;

b. have deteriorated performance due to the running of unauthorized software;

c. install and run software without the customers' knowledge and consent which can collect personal information, including end-users' search engine queries and results

from Microsoft's Bing search engine, that contain end-users' personal information; and

d. transmit collected personal information, including end-users' search engine queries that contain end-users' personal information, to the ZeroAccess Fraud Control IP Addresses and Fraud Control Domains.

48. The unauthorized access of and intrusion into Microsoft's Windows® operating system and Microsoft's customers' computers results in consumer confusion. To conduct the intrusion into end-user computers and ultimately to engage in click-fraud, Defendants cause the ZeroAccess Fraud Control IP Addresses to repeatedly use and cause the use of Microsoft's "Microsoft," "Windows," "Internet Explorer," and "Bing" trademarks in a confusing and misleading manner. Defendants use Microsoft's trademarks to cause the intrusion into the user's computer and to perform click-fraud by browser hijacking a user's computer and by using the user's computer to generate illegitimate automated traffic. This confuses the user into believing that Microsoft's Internet Explorer and Bing services and its Windows operating system are corrupt and untrustworthy, when they are not. Microsoft's customers have notified Microsoft of damage caused by the ZeroAccess botnet. Such customers have been confused and have been incorrectly led to believe that Microsoft was the source of damage, the ZeroAccess botnet's activity and the results of that activity, and therefore incorrectly attributed their injury to Microsoft and its products and services.

49. ZeroAccess also causes injury by defrauding Microsoft and Microsoft's advertiser customers. Internet advertiser customers who pay Microsoft and other ad service providers to increase targeted traffic to their websites expect that Microsoft's ad services make it more likely that end users searching for relevant items will visit their websites. ZeroAccess grossly skews and distorts this environment by generating non-user initiated clicks and website visits, increasing traffic to certain advertiser owner's websites and not others, and intercepting and diverting user-initiated actions. ZeroAccess' fraudulent traffic, however, does not lead to potential sales, misleading ad owners to pay advertisement distributors as if the ad owners' advertisements were legitimately clicked. Simply put, the ad owner paid for internet traffic that

is of no use. ZeroAccess also distorts the value of particular ad placements. The number of clicks an advertiser's ad receives determines, among other things, where an advertisers ad will be placed in the future. ZeroAccess changes the results on an infected end-user's computer and the advertiser's ad is not clicked. The advertiser is harmed because their ads are down-graded as less relevant, making it harder for their ads to get good placement on future search results. There is a substantial 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.

50. Thus, the ZeroAccess botnet and the ZeroAccess Fraud Control IP Addresses and Fraud Control Domains have caused injury to Microsoft's brand, reputation and goodwill. This incorrect attribution of the effects of the ZeroAccess botnet and ZeroAccess Fraud Control IP Addresses and Fraud Control Domains to Microsoft cause harm to Microsoft's brand and tarnishes the reputation of Microsoft's name, products and services. Microsoft has had to expend substantial resources in an attempt to assist its customers and to correct the continuing misperception that Microsoft is the source of damage caused by ZeroAccess botnet and the ZeroAccess Fraud Control IP Addresses and Fraud Control Domains.

51. Upon information and belief, Defendants who operate the ZeroAccess botnet benefit from its operation and the activities described above by operating as "traffic brokers," increasing visitors on specific websites through browser hijacking and automated traffic generation or by selling the hijacked traffic to other traffic brokers.

FIRST CLAIM FOR RELIEF

Violation of the Computer Fraud & Abuse Act, 18 U.S.C. § 1030

52. Microsoft realleges and incorporates by reference the allegations contained in paragraphs 1 through 51 above.

53. Defendants: (a) knowingly and intentionally accessed Microsoft customers' protected computers and Microsoft's protected computers without authorization or in excess of any authorization and thereby obtained information from the protected computers in a transaction

involving an interstate or foreign communication (18 U.S.C. § 1030(a)(2)(C)), (b) knowingly and with an intent to defraud accessed the protected computers without authorization or in excess of any authorization and obtained information from the computers, which Defendants used to further the fraud and obtain something of value (18 U.S.C. § 1030(a)(4)); (c) knowingly caused the transmission of a program, information, code and commands, and as a result of such conduct intentionally caused damage without authorization to the protected computers (18 U.S.C. § 1030(a)(5)(A)); and (d) intentionally accessed the protected computers without authorization, and as a result of such conduct caused damage and loss (18 U.S.C. § 1030(a)(5)(C)).

54. Defendants' conduct has caused a loss to Microsoft during a one-year period aggregating at least $5,000.

55. Microsoft has suffered damages resulting from Defendants' conduct.

56. Microsoft seeks compensatory and punitive damages under 18 U.S.C. § 1030(g) in an amount to be proven at trial.

57. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which Microsoft has no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

SECOND CLAIM FOR RELIEF

Violation of Electronic Communications Privacy Act, 18 U.S.C. § 2701

58. Microsoft realleges and incorporates by reference the allegations contained in paragraphs 1 through 51 above.

59. Microsoft's computers and servers and its licensed operating system are facilities through which electronic communication service is provided to its users and customers.

60. Defendants knowingly and intentionally accessed Microsoft customers' computers and Microsoft's computers and servers without authorization or in excess of any authorization granted by Microsoft.

61. Through this unauthorized access, Defendants had access to, obtained, altered, and/or prevented Microsoft's users' and customers' legitimate, authorized access to wire

electronic communications, including but not limited to user's search engine queries that contained personal information in electronic storage in the computers and servers of Microsoft and its customers and within Microsoft's licensed operating system.

62. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which Microsoft has no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

THIRD CLAIM FOR RELIEF

Trademark Infringement Under the Lanham Act – 15 U.S.C. § 1114 et. seq.

63. Microsoft realleges and incorporates by this reference each and every allegation set forth in paragraphs 1 through 51 above.

64. Defendants have used Microsoft's "Microsoft," "Windows," "Internet Explorer," and "Bing" trademarks ("Microsoft's Marks") in interstate commerce.

65. The Sirefef botnet generates and uses counterfeit copies of Microsoft's Marks in connection with Defendants' click-fraud by creating and distributing copies of Microsoft's Marks in counterfeit, manipulated version of Microsoft's Internet Explorer-branded browser and Microsoft's Bing-branded search engine webpage, and in fraudulent websites bearing Microsoft's Marks. By doing so, Defendants are likely to cause confusion, mistake, or deception as to the origin, sponsorship, or approval of the fake websites and the products and services promoted through the fake websites.

66. By using Microsoft's Marks in connection with Defendants' intrusion onto end-user computers and Defendants' click-fraud, Defendants have caused and are likely to cause confusion, mistake, or deception as to the origin, sponsorship, or approval of the fake websites generated and used by the ZeroAccess botnet. By doing so, Defendants have caused, and are likely to cause, confusion, mistake, or deception as to the origin, sponsorship, or approval of the conduct, actions, products and services carried out by or promoted by Defendants and the ZeroAccess botnet.

67. The ZeroAccess botnet creates keys and writes entries to the Windows® registry.

By creating keys and writing entries under a registry path that includes the Microsoft Marks, Defendants are likely to cause confusion, mistake, or deception as to the origin, sponsorship, or approval of the malicious software installed by the ZeroAccess botnet, including through the ZeroAccess IP addresses and domains.

68. As a result of their wrongful conduct, Defendants are liable to Microsoft for violating 15 U.S.C. § 1114.

69. Microsoft seeks injunctive relief and compensation and punitive damages in an amount to be proven at trial.

70. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which they have no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

71. Defendants' wrongful and unauthorized use of Microsoft's Marks to promote, market, or sell products and services constitutes trademark infringement pursuant to 15 U.S.C. § 1114 *et seq*.

FOURTH CLAIM FOR RELIEF

False Designation of Origin Under The Lanham Act – 15 U.S.C. § 1125(a)

72. Microsoft realleges and incorporates by this reference each and every allegation set forth in paragraphs 1 through 51 above.

73. The Microsoft Marks are distinctive marks that are associated with Microsoft and exclusively identify Microsoft's business, products, and services.

74. The ZeroAccess botnet generates and uses counterfeit copies of Microsoft's Marks in connection with Defendants' click-fraud by creating and distributing copies of Microsoft's Marks in counterfeit, manipulated version of Microsoft's Internet Explorer-branded browser and Microsoft's Bing-branded search engine webpage, and in fraudulent websites bearing Microsoft's Marks. By doing so, Defendants are likely to cause confusion, mistake, or deception as to the origin, sponsorship, or approval of the fake websites and the products and services promoted through the fake websites.

75. By using Microsoft's Marks in connection with Defendants' intrusion onto end-user computers and Defendants' click-fraud, Defendants have caused and are likely to cause confusion, mistake, or deception as to the origin, sponsorship, or approval of the fake websites generated and used by the ZeroAccess botnet. By doing so, Defendants have caused, and are likely to cause, confusion, mistake, or deception as to the origin, sponsorship, or approval of the conduct, actions, products and services carried out by or promoted by Defendants and the ZeroAccess botnet.

76. The ZeroAccess botnet creates keys and writes entries to the Windows® registry. By creating keys and writing entries under a registry path that includes the Microsoft Marks, Defendants are likely to cause confusion, mistake, or deception as to the origin, sponsorship, or approval of the malicious software installed by the ZeroAccess botnet, including through the ZeroAccess Fraud Control IP Addresses and Fraud Control Domains.

77. As a result of their wrongful conduct, Defendants are liable to Microsoft for violation of 15 U.S.C. § 1125(a).

78. Microsoft seeks injunctive relief and compensation and punitive damages in an amount to be proven at trial.

79. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which Microsoft has no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

FIFTH CLAIM FOR RELIEF

Trademark Dilution Under The Lanham Act – 15 U.S.C. § 1125(c)

80. Microsoft realleges and incorporates by this reference each and every allegation set forth in paragraphs 1 through 51 above.

81. The Microsoft Marks are distinctive marks that are associated with Microsoft and exclusively identify Microsoft's business, products, and services.

82. The ZeroAccess botnet generates and uses counterfeit copies of Microsoft's Marks in connection with Defendants' click-fraud by creating and distributing copies of

Microsoft's Marks in counterfeit, manipulated version of Microsoft's Internet Explorer-branded browser and Microsoft's Bing-branded search engine webpage, and in fraudulent websites bearing Microsoft's Marks. By doing so, Defendants are likely to cause dilution by blurring and dilution by tarnishment of the Microsoft Marks.

83. By using Microsoft's Marks in connection with Defendants' intrusion onto end-user computers and Defendants' click-fraud, Defendants have caused and are likely to cause dilution by blurring and dilution by tarnishment of the Microsoft Marks. By doing so, Defendants have caused, and are likely to cause dilution by blurring and dilution by tarnishment of the Microsoft Marks by improperly associating Microsoft's Marks with malicious conduct, actions, products and services carried out by or promoted by Defendants and the ZeroAccess botnet.

84. The ZeroAccess botnet creates keys and writes entries to the Windows® registry. By creating keys and writing entries under a registry path that includes the Microsoft Marks, Defendants are likely to cause dilution by blurring and dilution by tarnishment of the Microsoft Marks.

85. By using Microsoft's Marks falsely in connection with malicious activity, Defendants are likely to cause dilution by blurring and dilution by tarnishment of the Microsoft Marks, including through the ZeroAccess Fraud Control IP Addresses and Fraud Control Domains.

86. As a result of their wrongful conduct, Defendants are liable to Microsoft for violation of 15 U.S.C. § 1125(c).

87. Microsoft seeks injunctive relief and compensation and punitive damages in an amount to be proven at trial.

88. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which Microsoft has no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

SIXTH CLAIM FOR RELIEF

Common Law Trespass to Chattels

89. Microsoft realleges and incorporates by this reference each and every allegation set forth in paragraphs 1 through 51 above.

90. Defendants' actions in operating the ZeroAccess botnet result in unauthorized access to the computers and servers associated with Microsoft's Internet Explorer, Bing and Bing Ads services. Defendants actions in operating the ZeroAccess botnet result in unauthorized access to Microsoft's proprietary Windows operating system and customers' computers running that operating system, and result in an improper intrusion into those computers and operating systems, causing them to engage in click-fraud by sending the computers and Microsoft's Internet Explorer web browser sessions and Bing search engine results to websites of Defendants choice, without the authorization or consent of Microsoft or its customers.

91. Defendants intentionally caused this conduct and this conduct was unauthorized.

92. Defendants' actions have caused injury to Microsoft and its customers and imposed costs on Microsoft and its customers, including time, money and a burden on the computers of Microsoft and its customers, as well as injury to Microsoft's business goodwill and diminished the value of Microsoft's possessory interest in its computers and software.

93. As a result of Defendants' unauthorized and intentional conduct, Microsoft has been damaged in an amount to be proven at trial.

94. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which Microsoft has no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

SEVENTH CLAIM FOR RELIEF

Unjust Enrichment

95. Microsoft realleges and incorporates by this reference each and every allegation set forth in paragraphs 1 through 51 above.

96. The acts of Defendants complained of herein constitute unjust enrichment of the Defendants at Microsoft's expense in violation of the common law.

97. Defendants accessed, without authorization, computers running Microsoft's software.

98. Defendants used, without authorization or license, the facilities of Microsoft's software to, among other acts, deliver malicious software, support the ZeroAccess botnet and engage in click-fraud.

99. Defendants' actions in operating the ZeroAccess botnet result in unauthorized access to the computers and servers associated with Microsoft's Internet Explorer, Bing and Bing Ads services. Defendants actions in operating the ZeroAccess botnet result in unauthorized access to Microsoft's proprietary Windows operating system and customers' computers running that operating system, and result in an improper intrusion into those computers and operating systems, causing them to engage in click-fraud by sending the computers and Microsoft's Internet Explorer web browser sessions and Bing search engine results to websites of Defendants choice, without the authorization or consent of Microsoft or its customers.

100. Defendants profited unjustly from their unauthorized and unlicensed use of Microsoft's software and the computers of Microsoft and its customers by, among other things, diverting revenue from Microsoft's and its advertising customers and directing fraudulent Internet traffic to Microsoft's Bing Ads platform and through other means of monetization, defrauding Microsoft and its advertiser customers.

101. Defendants had an appreciation and knowledge of the benefit they derived from their unauthorized and unlicensed use of Microsoft's software and the computers of Microsoft and its customers, and the activities alleged herein.

102. Retention by the Defendants of the profits they derived from their unauthorized and unlicensed use of Microsoft's software and the computers of Microsoft and its customers, and the activities alleged herein, would be inequitable.

103. Defendants' unauthorized and unlicensed use of Microsoft's software and use of the computers of Microsoft and its customers, and the activities alleged herein, have damaged Microsoft in an amount to be proven at trial, and Defendants should disgorge their ill-gotten

profits.

104. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which Microsoft has no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

EIGHTH CLAIM FOR RELIEF

Conversion

105. Microsoft realleges and incorporates by this reference each and every allegation set forth in paragraphs 1 through 51 above.

106. Defendants have willfully interfered with and converted Microsoft's personal property, without lawful justification, as a result of which Microsoft has been deprived of possession and use of its property.

107. As a result of Defendants' actions, Microsoft has been damaged in an amount to be proven at trial.

108. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which Microsoft has no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Microsoft prays that the Court:

1. Enter judgment in favor of Microsoft and against the Defendants.

2. Declare that Defendants conduct has been willful and that Defendants have acted with fraud, malice and oppression.

3. Enter a preliminary and permanent injunction enjoining Defendants and their officers, directors, principals, agents, servants, employees, successors, and assigns, and all persons and entities in active concert or participation with them, from engaging in any of the activity complained of herein or from causing any of the injury complained of herein and from assisting, aiding or abetting any other person or business entity in engaging in or performing any of the activity complained of herein or from causing any of the injury complained of herein.

4. Enter a preliminary and permanent injunction preventing Defendants from using the ZeroAccess IP addresses and domains;

5. Enter judgment awarding Microsoft actual damages from Defendants adequate to compensate Microsoft for Defendants' activity complained of herein and for any injury complained of herein, including but not limited to interest and costs, in an amount to be proven at trial.

6. Enter judgment disgorging Defendants' profits.

7. Enter judgment awarding enhanced, exemplary and special damages, in an amount to be proved at trial.

8. Enter judgment awarding attorneys' fees and costs, and

9. Order such other relief that the Court deems just and reasonable.

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