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

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

AMENDED COMPLAINT

Plaintiff MICROSOFT CORP. ("Microsoft") hereby complains and alleges against MARAT MAZYNSKIJ ("Mazynskij") and DMITRY CHUPAKHIN ("Chupakhin") (referred to collectively herein as "Defendants"), controlling the "Bamital" botnet using the Internet domains and Internet Protocol (IP) addresses set forth at Appendices A, B, and C to this Complaint ("the Bamital IP addresses and 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 "Bamital" botnet, by means of the Bamital IP addresses and 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. Defendant Marat Mazynskij has procured and controlled Bamital domains and IP addresses set forth in Appendices A, B and C, that have been misused to cause harm to Microsoft, its customers, and the public. Microsoft is informed and believes and thereupon alleges that Marat Mazynskij resides at Kosmoso 16-11, Visaginas LT-31104, Lithuania and/or in Minsk, Belarus, and can be contacted at email addresses: zipmonstr@gmail.com, mmazynskij@gmail.com, marat@tts.lt, pakovelli@yahoo.com, davidzonbigid@gmail.com, taxi.1979@mail.ru, trusart88@gmail.com, viktorhamov@yahoo.com, viktorhamov2@yahoo.com, todeallr@yahoo.com, auselloyosjuv@gmail.com, billsberryhok@gmail.com, peter1979@qmail.com, alexsmit2011@gmail.com, seven2011@gmail.com, rosannaleazuk@gmail.com, s15051575@yandex.ru, s15@mail.ru, tarosmit@yandex.ru, worldsearch@yandex.ru, martiula2@bk.ru.

4. Defendant Dmitry Chupakhin aka "Sergey Skorovod" has procured and controlled Bamital domains set forth in Appendices A, B and C, that have been misused to cause harm to Microsoft, its customers, and the public. Microsoft is informed and believes and thereupon alleges that Dmitry Chupakhin resides at Barbyusa St., Bldg. 134, apt. 24, Chelyabinsk 454078, Russian Federation and can be contacted at email addresses: serg.skorovod@gmail.com, pizdato77@gmail.com.

5. Defendants own, operate, control and maintain the Bamital botnet and do business under the names of the Bamital domains and IP addresses.

6. Microsoft will exercise due diligence to effect service upon Defendants.

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

8. Defendants have provided the contact information for the Bamital domains and IP addresses set forth at Appendices A, B, and C to this Complaint, including falsified information.

9. Third party National Internet Exchange of India is a regional name registry in India that oversees the registration of all domain names ending in ".in," including all of the Bamital ".in" domains, and is located at 5th Floor Incube Business Centre, 18, Nehru Place, New Delhi, Delhi 110 019, India. The National Internet Exchange of India contracts its registry responsibilities for the ".in" domains through Afilias Limited, Afilias U.S.A., Inc. and related entities (collectively "Afilias"), which is located at 300 Welsh Road, Building 3, Suite 105, Horsham, Pennsylvania 19044. Third party Afilias is the domain name registry that oversees the registration of all domain names ending in ".info," including all of the Bamital ".info" domains.

10. 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," ".net" and ".cc" including all of the Bamital ".com," ".net" and ".cc" 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.

11. Third party Public Interest Registry ("PIR") is the domain name registry that oversees the registration of all domain names ending in ".org" including the Bamital ".org" domains. PIR is located at 1775 Wiehle Avenue, Suite 200, Reston, Virginia 20190.

12. Third party Kim Jong Sung is the administrator of the domain .co.cc, misused by Defendants in this case to control the Bamital botnet, and has operated subdomain services through that domain directed at the United States and the Eastern District of Virginia. Kim Jong Sung is located at 864-2, Janghangdong, Ilsan, Goyang, Gyeounggi 410837, South Korea.

13. Third party Dominique Piatti is the administrator of the domains cz.cc and uni.me, misused by Defendants in this case to control the Bamital botnet, and operates subdomain services through those domains directed at the United States and the Eastern District of Virginia. Dominique Piatti is located at Prazska 636, Dolni Brezany, Praha-Zapa 25241, Czech Republic.

14. Third party Martin Semrad and i-Registry s.r.o. are the administrators of the domain

co.cz , misused by Defendants in this case to control the Bamital botnet, and operates subdomain services through that domain directed at the United States and the Eastern District of Virginia. Martin Semrad and i-Registry s.r.o. are located at Nad výpustí 142, Praha 4 14900, Czech Republic.

15. Third parties ISPrime LLC and ISPrime, Inc. (collectively "ISPrime") are Internet service providers and hosting companies. As part of their Internet services, ISPrime provides IP addresses to their customers. Bamital IP address 64.111.211.169 listed in Appendix B and underlying domains at issue in this case, is designated as an IP address maintained by ISPrime. ISPrime is located at 300 Boulevard East, Suite 100, Weehawken, New Jersey 07086-6702.

16. Third parties Leaseweb USA, Inc. and Leaseweb B.V. (collectively "Leaseweb") are Internet service providers and hosting companies. As part of their Internet services, Leaseweb provides IP addresses to their customers. Bamital IP addresses 85.17.239.25, 82.192.79.26, and 88.192.88.13 listed in Appendix B and underlying domains at issue are designated as IP addresses maintained by Leaseweb. Leaseweb USA, Inc. is located at 9480 Innovation Drive, Suite 1, Manassas, Virginia 20110. Leaseweb B.V. is located at Mollerusweb 102, 2031 BZ Haarlem, The Netherlands and P.O. Box 93054, 1090 BB Amsterdam, The Netherlands.

17. 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 and/or others 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 others, 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 and others.

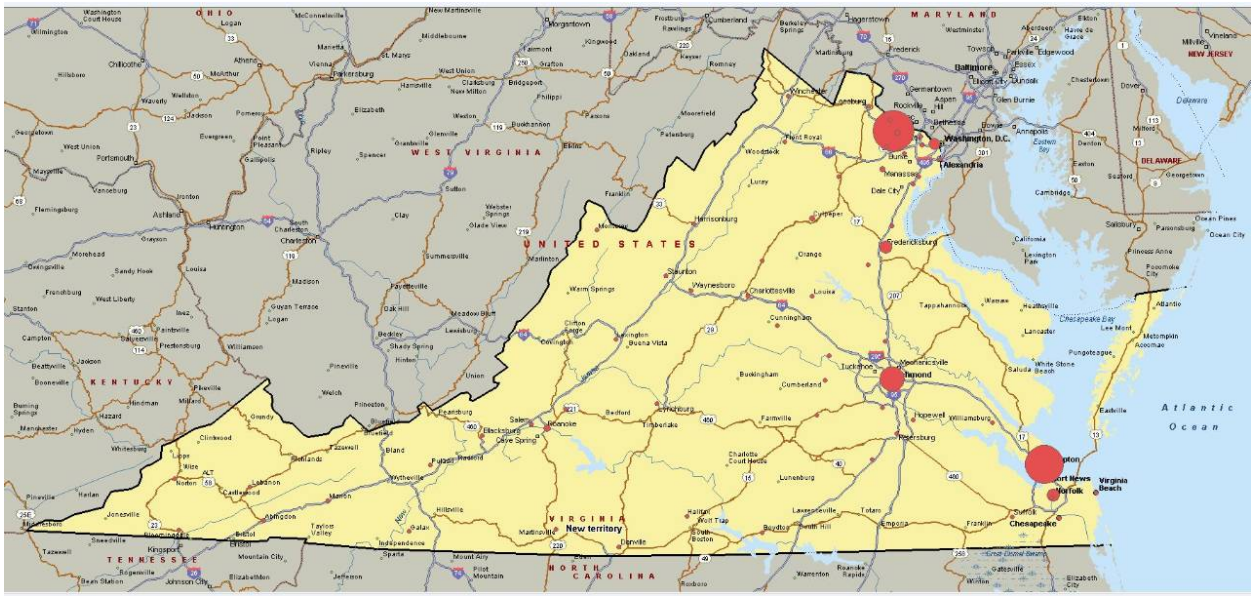
JURISDICTION AND VENUE

18. 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 and conversion. Accordingly, this Court has subject matter jurisdiction under 28 U.S.C. § 1367.

19. 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 Virginia and the Eastern District of Virginia to carry out the acts complained of herein.

20. Defendants have affirmatively directed actions at Virginia and the Eastern District of Virginia by directing malicious computer code at the computers of individual users located in Virginia and the Eastern District of Virginia, 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 depicts the geographical location of user computers in Virginia and the Eastern District of Virginia against which Defendants are known to have directed malicious code, attempting to infect those computers and enlist them in the botnet:



21. Defendants also maintain Bamital IP addresses specifically registered through

Leaseweb, with a presence in the Eastern District of Virginia. Defendants maintain Bamital ".com," ".net," ".cc" and ".org," Internet domains registered respectively through Verisign and PIR in the Eastern District of Virginia. Defendants harm Microsoft, its customers, and the public through the Bamital domains and IP addresses by using those domains and IP addresses to control the communications of a network of compromised user computers, called a "botnet," which Defendants own, operate, and maintain.

22. Defendants have undertaken the acts alleged herein with knowledge that such acts would cause harm through the ".com," ".net," and ".org" domains located in the Eastern District of Virginia, through IP addresses maintained through facilities in the Eastern District of Virginia and through user computers located in the Eastern District of Virginia, thereby injuring Microsoft, its customers, and others both in the Eastern District of Virginia and elsewhere in the United States. Therefore, this Court has personal jurisdiction over Defendants.

23. 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(b) because a domain name is deemed to have its situs in the judicial district in which the domain name registry that registered or assigned the domain name is located. Verisign and PIR are domain name registries for the Bamital domains located in this district. Leaseweb is an Internet service provider for the Bamital IP addresses located in this 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

24. 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 D to this Complaint.

Internet Advertising And Click-fraud

25. Online advertising is a multibillion dollar a year industry with U.S. online advertising expenditures reaching $12.7 billion in 2012, and growing at 17% 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. These schemes require cybercriminals to devise methods of gaining control over end-user computers, typically by infecting the computers with malicious software, known as "malware."

26. 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.

27. An end 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.

28. 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.

29. 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.

30. 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."

31. 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.

32. 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"

33. In general, 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 the software (known as malicious software or malware) that makes the computer part of the botnet. For example, an end-user's computer may become part of a botnet when the user inadvertently interacts with a malicious website advertisement, clicks on a malicious email attachment or downloads malicious software. In each such instance, software code is downloaded or executed on the user's computer, causing that computer to become part of the botnet, capable of sending and receiving communications, code and instructions to or from other botnet computers.

34. 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.

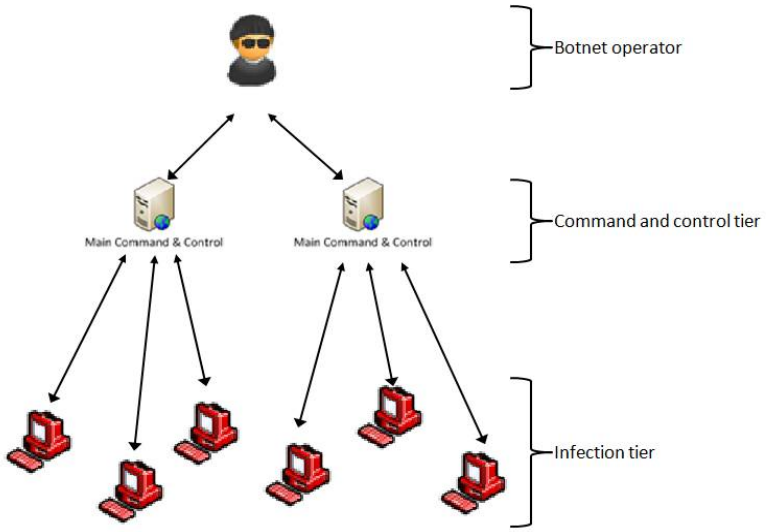
35. Botnets are often created and controlled by sophisticated criminal organizations and are used to carry out misconduct that harms others' rights. For example, a computer in a botnet

may be used to anonymously send unsolicited, bulk email without the knowledge or consent of the individual user who owns the compromised computer. Similarly, a botnet computer may be used to deliver further malicious software that infects other computers, making them part of the botnet as well. A botnet computer may also be used 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, in order to obscure and conceal the true source of those communications.

The "Bamital" Botnet: Overall Architecture

36. 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 "Bamital" botnet.

37. The Bamital botnet has a multi-tiered architecture, which can be represented as follows:



38. The lowest "**infection-tier**" in this architecture is estimated to be comprised of multiple thousands of Bamital-infected end-user computers that might be office or home desktop computers, laptop computers, or computers in public libraries. These infected user computers are essentially the workers of the botnet, performing the day-to-day illegal activity, including click-fraud. Functionally, the Bamital malware has 3 major components – "main module," "module a," and "module c." Each module communicates with a set of specialized Bamital command and

control servers hosted at the Bamital domains and IP addresses.

39. Defendants use deceptive methods to infect end-user computers. Upon information and belief, Defendants controlling the Bamital botnet are part of an anonymous group of cybercriminals that have created websites designed specifically to infect end-user computers. When unsuspecting users browse one of these websites, the user's computer is taken to another website where malware called an "exploit pack" (usually the "Phoenix" 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 Bamital malware. Upon information and belief, Defendants' websites propagating Bamital are part of an organized effort to infect victims' users and are not a random assortment of websites. Specifically, all Bamital websites install a small text file known as a "cookie" on the user's computer so that Defendants can identify computers that are already probed and infected. The cookie includes the text "yatutuzebil" – a Russian phrase loosely translating to "I was already here."

40. Once infected, Defendants direct Bamital-infected end-user computers to engage in click-fraud either through hijacking the web browsers of the Bamital-infected end-user computers or by instructing the infected computers to generate automated Internet traffic. Bamital's modular structure allows Defendants to use Bamital-infected end-user 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 Bamital-infected computers are unaware that their machines are infected and operating as part of the Bamital botnet.

41. At the highest tier in the architecture, the "**command and control tier**" consists of domains and IP addresses that are used as command and control servers to continuously control the Bamital-infected end-user computers. Command and control servers refer to either physical server computers or software running on computers that support the Bamital botnet. The number and location of the command and control servers may change over time. Upon information and belief, these servers are also controlled directly by the operators of the Bamital botnet and not made up of infected computers.

The Bamital Botnet's Domains And IP Addresses

42. The Bamital botnet uses primarily three groups of command and control servers. Bamital's main command and control servers control the ability of the Bamital infected end-user computers to communicate with each other and to expand the botnet. The main command and control servers send infected end-user computers information and instructions over the Internet that force the Bamital-infected end-user computers to engage in "click-fraud." The Bamital malware's main module contains an algorithm that generates names of possible domain names that the Bamital botnet controllers may use as command and control servers. Using the current date as the initial input, the domain name generation algorithm generates five domains and appends each of the five domains with domain suffixes generating 15 domains daily. Bamital's main module connects the infected user's computer to the Internet and attempts to establish contact with the 15 domains in order to receive its next set of instructions. Defendants run the same domain name generation algorithm, then register some or all of the domain names, and then place instructions at those domains to interact with the infected user computers.

43. **Appendix A** lists the domains hosting the Bamital's main command and control server domains generated by the name generation algorithms, some of which are already registered and some of which are reserved by Defendants to register in the future to control the botnet. The purpose of each of the Bamital domains set forth in Appendix A is to support and propagate the Bamital botnet and further its malicious activity.

44. Defendants use the Bamital botnet to engage in click-fraud by hijacking Bamital-infected end-user computers. Bamital's malware's module "a" is responsible for "**browser hijacking**" which occurs when the Bamital malware takes control of an infected end-user's web browser and redirects the user to a search website of the botnet operator's choosing. Bamital's module "a" 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. Once a user clicks on any of the search links, Bamital's module "a" takes control of the user's Internet Explorer browser and Bing search

results and redirects Internet Explorer and the Bing search results to a specialized Bamital command and control servers – module "a" command and control servers – and then redirects the user to one of several possible websites predetermined by the Defendants. These websites to which users are redirected are not websites associated with the link the user clicked on and are not the destination intended by the user, Microsoft or its advertising partners. The Bamital module "a" command and control servers hijack the normal Internet Explorer browser functionality and the Bing search functionality and misrepresent to the user that they are using the Microsoft's Internet Explorer-branded browser and Bing-branded search engine containing Microsoft's Internet Explorer and Bing trademarks. In reality, the module "a" command and control server redirects the user's Internet Explorer browser and Bing search to websites predetermined by the botnet operators.

45. **Appendix B** lists domains and IP addresses hosting the Bamital's module "a" command and control servers. Some of the domains are already registered and some are reserved by Defendants to register in the future to control the botnet. The purpose of each of the Bamital domains and IP addresses set forth in Appendix B is to support and propagate the Bamital botnet and further its malicious activity.

46. The Bamital malware can also force infected end-user computers to generate automated internet traffic by instructing those computers – without the user's knowledge or intervention – to connect to any website that Defendants choose. Bamital's module "c" communicates with the Bamital's module "c" command and control servers and instructs the infected end-user computers to download a list of target websites. Module "c" then launches a "hidden" instance of a web browser – such as Microsoft's Internet Explorer – on the infected end-user computers and causes the hidden browser to visit those websites that Defendants have chosen as though it were a real user. 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 module "c" forces the infected computer to perform. The module "c" command and control server can point the infected end-user computer to new command and

control servers or begin the process of queuing websites to be visited. Module "c" will report to the module "c" command and control server to ensure the fraudulent traffic is logged. Module "c" contains one or more predetermined domain names of the module "c" command and control servers.

47. **Appendix C** lists the domains hosting the Bamital's module "c" command and control servers. Some of the domains are already registered and some the domains are reserved by Defendants to register in the future to control the botnet. The purpose of each of the Bamital domains set forth in Appendix C is to support and propagate the Bamital botnet and further its malicious activity.

Injury Caused By The Bamital Botnet To Microsoft And Its Customers

48. The malicious Bamital botnet software 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. In particular, the Bamital botnet specifically targets the Windows® operating system, including at least the following files in the Windows operating system: iexplore.exe, explorer.exe, winlogon.exe, spoolsv.exe, svchost.exe, sysprep.exe, wmiprvse.exe. The Bamital botnet, for example, writes particular entries to the registry of the 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 spread of the Bamital botnet in this way is not related to any vulnerability in Microsoft's systems, but is instead achieved by misleading unwitting users into taking steps that result in the infection of their machines.

49. The Bamital 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 Bamital botnet.

50. The Bamital botnet harms Microsoft's customers by misusing the Windows®

operating system on those users' infected computers. The Bamital 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 Bamital command and control servers.

51. 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 Bamital command and control servers 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 Bamital botnet. Such customers have been confused and have been incorrectly led to believe that Microsoft was the source of damage, the Bamital botnet's activity and the results of that activity, and therefore incorrectly attributed their injury to Microsoft and its products and services.

52. Bamital 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. Bamital 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. Bamital's 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. Bamital also distorts the value of particular ad placements. The number of clicks an advertiser's ad receives determines, among other things, where an advertiser's ad will be placed in the future. Bamital 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.

53. Thus, the Bamital botnet and the Bamital IP addresses and domains have caused injury to Microsoft's brand, reputation and goodwill. This incorrect attribution of the effects of the Bamital botnet and Bamital domains and IP addresses to Microsoft causes 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 the Bamital botnet and the Bamital IP addresses and domains.

54. Upon information and belief, Defendants who operate the Bamital 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

55. Microsoft realleges and incorporates by reference the allegations contained in

paragraphs 1 through 54 above.

56. 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)).

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

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

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

60. 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

61. Microsoft realleges and incorporates by reference the allegations contained in paragraphs 1 through 54 above.

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

63. 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.

64. 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.

65. 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.*

66. Microsoft realleges and incorporates by this reference each and every allegation set forth in paragraphs 1 through 54 above.

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

68. The Bamital 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.

69. 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 Bamital 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 Bamital botnet.

70. The Bamital 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 Bamital botnet, including through the Bamital IP addresses and domains.

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

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

73. 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.

74. 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)

75. Microsoft realleges and incorporates by this reference each and every allegation set forth in paragraphs 1 through 54 above.

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

77. The Bamital 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.

78. 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 Bamital 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 Bamital botnet.

79. The Bamital 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 Bamital botnet, including through the Bamital IP addresses and domains.

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

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

82. 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)

83. Microsoft realleges and incorporates by this reference each and every allegation set forth in paragraphs 1 through 54 above.

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

85. The Bamital 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.

86. 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 Bamital botnet.

87. The Bamital 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.

88. 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 Bamital IP addresses and domains.

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

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

91. 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

92. Microsoft realleges and incorporates by this reference each and every allegation set forth in paragraphs 1 through 54 above.

93. Defendants' actions in operating the Bamital 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 Bamital 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.

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

95. 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.

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

97. 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

98. Microsoft realleges and incorporates by this reference each and every allegation set forth in paragraphs 1 through 54 above.

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

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

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

102. Defendants' actions in operating the Bamital 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 Bamital 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.

103. 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.

104. 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.

105. 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.

106. 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.

107. 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

108. Microsoft realleges and incorporates by this reference each and every allegation set forth in paragraphs 1 through 54 above.

109. 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.

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

111. 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 giving Microsoft control over the Bamital botnet and the Bamital botnet domains and IP addresses in order to cause injury caused by those instrumentalities to cease, preserving evidence of Defendants' misconduct and ordering means by which Microsoft may inform victim end-users that their computers are infected and provide resources to remove the Bamital malware from those computers.

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: June 17, 2013

Respectfully submitted,

ORRICK, HERRINGTON & SUTCLIFFE LLP

/s/ Lauren Parker

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

Of counsel:

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

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

DEMAND FOR JURY TRIAL

Microsoft respectfully requests a trial by jury on all issues so triable in accordance with Fed. R. Civ. P. 38.

Dated: June 17, 2013

Respectfully submitted,

ORRICK, HERRINGTON & SUTCLIFFE LLP

/s/ Lauren Parker

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

Of counsel:

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

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