

FILED

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

2015 FEB 20 A 9:20

MICROSOFT CORPORATION, a
Washington corporation, and FS-
ISAC, INC., a Delaware corporation,

Plaintiffs,

v.

JOHN DOES 1-3, CONTROLLING
A COMPUTER BOTNET THEREBY
INJURING PLAINTIFFS AND
THEIR CUSTOMERS AND
MEMBERS,

Defendants.

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

Civil Action No: 1:15 cv 240 LMB/IDD

**FILED UNDER SEAL PURSUANT
TO LOCAL CIVIL RULE 5**

COMPLAINT

Plaintiffs MICROSOFT CORP. ("Microsoft") and FS-ISAC, INC., ("FS-ISAC") hereby complain and allege that JOHN DOES 1-3 (collectively "Defendants") have illegally created and are using for criminal purposes a global network of interconnected computers known as the "Ramnit botnet" or "Ramnit." Ramnit is comprised of user computers connected to the Internet that Defendants have infected with malicious software. Defendants have used and continue to use Ramnit to steal millions of dollars from the users of the infected computers and from the financial institutions with which those users conduct financial transactions over the Internet. Defendants control Ramnit through a command and control infrastructure hosted at and operated through the Internet domains set forth at Appendix A to this Complaint (the "domains") (the "Ramnit Command and Control Infrastructure"). Plaintiffs allege 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; (8) Conversion; and (9) intentional interference with contractual relationships. Plaintiffs seek injunctive and other equitable relief and damages against Defendants who operate and control a network of computers known as the “Ramnit” botnet through the Ramnit Command and Control Infrastructure. Defendants, through their illegal activities involving Ramnit, have caused and continue to cause irreparable injury to Plaintiffs, their member organizations and 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. Plaintiff FS-ISAC, Inc. is a non-profit corporation duly organized and existing under the laws of Delaware, having its headquarters and principal place of business in Reston, Virginia. FS-ISAC is a membership organization comprised of 5,200 organizations including commercial banks and credit unions of all sizes, brokerage firms, insurance companies, payment processors, and over 20 trade associations representing the majority of the U.S. financial services sector. FS-ISAC represents the interests of its financial services industry members in combating and defending against cyber threats that pose risk and loss to the industry.

4. On information and belief, **John Doe 1** controls the Ramnit botnet in furtherance of conduct designed to cause harm to Plaintiffs, their customers, and the public. Plaintiffs are informed and believe and thereupon allege that John Doe 1 can likely be contacted directly or through third-parties using the information set forth in Appendix A.

5. On information and belief, **John Doe 2** controls the Ramnit botnet in furtherance of conduct designed to cause harm to Plaintiffs, their customers, and the public. Plaintiffs are informed and believe and thereupon allege that John Doe 2 can likely be contacted directly or through third-parties using the information set forth in Appendix A.

6. On information and belief, **John Doe 3** controls the Ramnit botnet in furtherance of conduct designed to cause harm to Plaintiffs, their customers, and the public. Plaintiffs are

informed and believe and thereupon allege that John Doe 3 can likely be contacted directly or through third-parties using the information set forth in Appendix A.

7. Third parties VeriSign Naming Services and VeriSign Global Registry Services (collectively, "VeriSign") are the domain name registries that oversee the registration of all domain names ending in ".com." 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.

8. Set forth in Appendix A are the identities of and contact information for third party domain registries that control the domains used by the Defendants.

9. On information and belief, John Does 1-3 jointly own, rent, lease, or otherwise have dominion over the Ramint botnet and Ramnit Command and Control Infrastructure and control, maintain, and do business through the Ramnit botnet and the Ramnit Command and Control Infrastructure. Plaintiffs will amend this complaint to allege the Doe Defendants' true names and capacities when ascertained. Plaintiffs will exercise due diligence to determine Doe Defendants' true names, capacities, and contact information, and to effect service upon those Doe Defendants.

10. Plaintiffs are informed and believe and thereupon allege that each of the fictitiously named Doe Defendants is responsible in some manner for the occurrences herein alleged, and that Plaintiffs' injuries as herein alleged were proximately caused by such Defendants.

11. On information and belief, the actions and omissions alleged herein to have been undertaken by John Does 1-3 were actions that Defendants, and each of them, 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 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 Defendant 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

12. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because 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). The Court also has subject matter jurisdiction over Plaintiffs' claims for trespass to chattels, unjust enrichment, and conversion pursuant to 28 U.S.C. § 1367.

13. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to Plaintiffs' claims has occurred in this judicial district, because a substantial part of the property that is the subject of Plaintiffs' claims is situated in this judicial district, and because a substantial part of the harm caused by Defendants has occurred in this judicial district. Defendants maintain Internet domains registered in Virginia, engage in other conduct availing themselves of the privilege of conducting business in Virginia, and have utilized instrumentalities located in Virginia and the Eastern District of Virginia to carry out the acts of which Plaintiffs complain.

14. 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, and attempting to and in fact infecting those user computers with the malicious code to make the user computers part of the Ramnit botnet, which is used to injure Plaintiffs, their customers, and the public. **Figure 1**, below, depicts the geographical location of user computers in and around the Eastern District of Virginia, against which Defendants are known to have directed malicious code, attempting to and in fact infecting those computers, thereby enlisting them into the Ramnit botnet:

Fig. 1



15. Defendants maintain certain of the Ramnit Domains registered through VeriSign which resides in the Eastern District of Virginia. Defendants use these domains to communicate with and control the Ramnit-infected computers that Defendants communicate with, control, steal from, update, and maintain in this judicial district. Defendants have undertaken the acts alleged herein with knowledge that such acts would cause harm through domains located in the Eastern District of Virginia, through the Ramnit domains maintained through facilities in the Eastern District of Virginia, and through user computers located in the Eastern District of Virginia, thereby injuring Plaintiffs, the customers and member organizations of Plaintiffs, and others in the Eastern District of Virginia and elsewhere in the United States. Therefore, this Court has personal jurisdiction over Defendants.

16. 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 Plaintiffs' claims, together with a substantial part of the property that is the subject of Plaintiffs' claims, are situated in this judicial district. Venue is proper in this judicial district under 28 U.S.C. § 1391(c) because Defendants are subject to personal jurisdiction in this judicial district.

FACTUAL BACKGROUND

Plaintiffs' Services And Reputation

17. Microsoft® is a provider of the Windows® operating system and the Internet Explorer® web browser, 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 Microsoft®, Windows®, and Internet Explorer®. Copies of the trademark registrations for the Microsoft, Windows, and Internet Explorer trademarks are attached as Appendix B to this Complaint.

18. Plaintiff FS-ISAC is a trade organization comprised of 5,200 organizations including commercial banks and credit unions of all sizes, brokerage firms, insurance companies, payment processors, and over 20 trade associations representing the majority of the U.S. financial services sector. It was established by the financial services sector in response to the 1998 Presidential Directive 63, later updated by the 2003 Homeland Security Presidential Directive 7, which requires that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect the United States' critical infrastructure. (*See* www.fsisac.com/about/). Its purpose is "to enhance the ability of the financial services sector to prepare for and respond to cyber and physical threats, vulnerabilities and interests...." FS-ISAC's activities include actively coordinating and promoting financial industry detection, analysis, and response to cybersecurity threats. FS-ISAC works closely with various government agencies including the U.S. Department of Treasury, Department of Homeland Security (DHS), Federal Reserve, Federal Financial Institutions Examination Council regulatory agencies, United States Secret Service, Federal Bureau of Investigation, and other state and federal agencies. Financial institutions that are members of FS-ISAC have generated

substantial goodwill with their customers, establishing a strong brand and developing their respective names and the names of their products and services into strong and famous world-wide symbols that are well-recognized within their channels of trade.

Computer “Botnets”

19. A “botnet” is a collection of individual computers infected with malicious software (“malware”) that allows communication among those computers and centralized or decentralized communication with other computers providing control instructions. A botnet network may be comprised of hundreds of thousands and sometimes millions, of infected user computers. The individual computers in a botnet often belong to users who have unknowingly downloaded or been infected by the malware. 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 a document that contains hidden malware. In each instance where Ramnit malware is downloaded and successfully executed on the user’s computer, it causes that computer to become part of the Ramnit botnet. Once part of a botnet, the user’s computer is capable of sending and receiving communications, code, and instructions to or from other botnet computers.

20. Many botnets are controlled through a set of specialized server computers referred to as “command and control computers.” The command and control servers are often wholly under the control of the botnet creators. These may have specialized functions, such as sending control instructions to infected user computers or uploading stolen information from them.

21. Criminal organizations and individual cybercriminals usually create, control, maintain, and propagate botnets in order to carry out misconduct that harms others’ rights. Cybercriminals favor the use of botnets for many illegal activities because botnets support a wide range of illegal conduct, are difficult for security experts to disable or eradicate, and conceal the identities of the malefactors controlling them. The controllers of a botnet will use an infected user computer for a variety of illicit purposes, unknown to the end user. A computer in a botnet, for example, may be used to:

- a. carry out theft of money, credentials, or other sensitive information or

- engage in fraud, computer intrusions, or other misconduct;
- b. anonymously send unsolicited bulk email without the knowledge or consent of the individual user who owns the compromised computer;
- c. deliver further malware to infect other computers; or
- d. “proxy” or relay Internet communications originating from other computers, in order to obscure and conceal the true source of those communications.

22. Botnets provide a very efficient means of controlling a large number of computers for illegal purposes and a means of targeting any illicit action against the contents of those computers, the users of those computers, or against computers and networks connected to the Internet.

Overview Of The Ramnit Botnet

23. Plaintiffs bring this action to stop Defendants from harming Plaintiffs, the customers and member organizations of Plaintiffs, and the public, through the Ramnit Command and Control Infrastructure, which is central to the illegal operation of the Ramnit botnet.

24. Defendants use the Ramnit botnet primarily to gain access to personal account credentials, including passwords and user names for online financial websites. Defendants use these credentials to steal—among other things—funds from the computer users and from the financial institutions of which those users are customers. When a user of a Ramnit-infected computer attempts to log onto a financial institutions website, Ramnit captures the user’s online financial login credentials and other personal identifying information, and sends that information to Defendants for later exploitation.

25. Ramnit may even add additional questions and prompts to the webpage of a financial institution as it is displayed on the user’s computer so as to extract additional account credential information from the user. The method Defendants use to achieve this scheme is commonly referred to as a “web inject.” Each Ramnit bot maintains a list of financial institutions to be targeted in this manner.

26. In addition to using web injects as described above, Ramnit also includes a

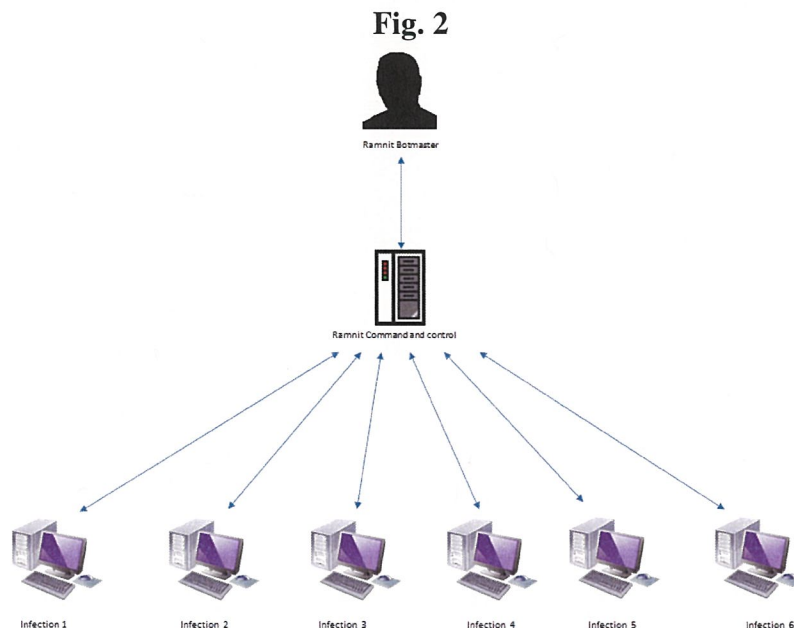
malware module that searches documents on an infected computer's hard drive, looking for words such "account," "password," "credit card," or the names of targeted financial institutions. The Ramnit malware detects such documents and sends them to Defendants for review and potential exploitation.

27. The user is unaware of Ramnit's activity as Defendants have designed Ramnit to hide itself and its unlawful activity on infected computers in part by disabling the security defenses of the user's computer. The operating system still purports to be Windows, and the browser still purports to be the user's normal browser, be it Internet Explorer, Chrome, Firefox, or other. But in fact, Ramnit has corrupted and thereby converted these products into instruments of fraud aimed directly at the user of the computer. The typical user is unaware of Defendants' surveillance and control of her computer and theft of her identity and of funds from her account.

28. After Ramnit captures the user's login credentials and personal identifying information, Defendants use that information, for example, to access the user's bank account.

The Ramnit Botnets' Infrastructure

29. The Ramnit botnets have a multi-tiered architecture that is represented in **Figure 2**, below:



30. The lowest tier of computers is referred to as the **“Infection Tier.”** This is comprised of tens and possibly hundreds of thousands of Ramnit-infected user computers. These computers may be home desktop computers, laptop computers, or computers in public libraries. These infected user computers are essentially the workers of the Ramnit botnet, performing the day-to-day illegal activity, including the theft of sensitive credentials from any person using the computer.

31. Defendants use deceptive methods to infect user computers. Upon information and belief, Defendants controlling the Ramnit botnet are part of a criminal enterprise that have infected legitimate websites and/or created websites designed specifically to infect user computers. When an unsuspecting user browses one or more of these websites, the user’s computer is linked over the Internet to another website where an “exploit pack” is downloaded and silently probes the user’s computer for vulnerabilities, looking for an opportunity to execute code or place the malware onto the system.

32. Defendants have been alarmingly successful in spreading the Ramnit infection to computers around the world. Since approximately January 2010, Ramnit has been among the most prolifically spread malware infections among the many that are tracked by security experts.

33. Once infected, Defendants direct the Ramnit-infected computers to engage in unlawful conduct, including (a) stealing users’ online login credentials for financial institutions and other online accounts; (b) stealing users’ personal identifying information; (c) stealing funds from users and financial institutions; (d) hijacking users’ web browsers; (e) surveying users’ computers for other sensitive information; as well as other illegal activity. Most if not all owners of Ramnit-infected computers are unaware that their machines are infected and operating as part of the Ramnit botnets.

The Ramnit Command And Control Infrastructure

34. Defendants control the computers in the Infection Tier through infrastructure that serves as the botnet’s **“Command and Control Tier.”** The Command and Control Tier consists of domains (more commonly referred to as websites), computers hosting the domains, and IP addresses at which those computers connect to the Internet. Command and control servers refer

to either physical server computers or software running on computers that support the Ramnit botnets. Defendants use and control these command and control servers to continuously control the Ramnit-infected computers.

35. When first installed on a user's computer, the Ramnit malware generates a list of 300 random domain names (i.e., website names) via a custom algorithm. After it generates the list of 300 domain names, it will next begin to attempt to contact each one in turn over the Internet, and will continue cycling through its list until one of the domains for a command and control server responds authoritatively with a Ramnit-encrypted command.

36. Defendants generate the exact same list of domain names as have the infected computers. To communicate with the Ramnit bots, the Defendants register at least one of the domains in the list of 300 domains, associating the domain name with a numeric IP address and a command and control computer located at the IP address. Remotely, over the Internet, Defendants can then place further instructions or malware on that command and control computer for the bots to download, and can receive information uploaded by the bots.

Defendants Use The Ramnit Botnets To Steal Money

37. The Ramnit botnets' primary goal is to steal financial account credentials of owners of Ramnit-infected computers to allow Defendants to access owners' financial accounts and siphon funds to Defendants. Defendants, through the Ramnit botnets, use multiple techniques to conduct those attacks.

38. For example, the Ramnit botnets' malware running on the infected computers can engage in a "web-inject" attack to extract sensitive information from the user. In a web-inject attack, Ramnit alters the appearance of the financial institutions' webpage as it is being displayed in the user's web browser. Instead of allowing the browser to provide an accurate rendering of the financial website, Ramnit causes the browser to change what the user sees. It does this by "injecting" additional code into the website code that the browser is rendering in a displayable format for the user. For example, if the real website asks only for a login ID and password, Ramnit can extend it through a web-inject and ask for additional information such as social security number, birth date, mother's maiden name, and other such information typically used to

answer security questions. Again, Ramnit will record this information and upload it later to Defendants, who can use it to steal from the user. In this way, Ramnit intercepts communications between the financial institution's website and the user. Ramnit is capable of exploiting various browsers in this manner including, for example, Microsoft Internet Explorer and Mozilla Firefox.

39. Defendants repeatedly misuse the trademarks of financial institutions on these fake online banking websites in order to confuse and mislead victims. Critically, through the web injection attack, Ramnit effectively replaces the real webpage with a corrupted and sabotaged webpage, but it keeps the trademarks of the FS-ISAC member institution which it happens to be targeting. Defendants design the web-injects to use those trademarks in such a manner to mimic the real website of a financial institution. This confuses owners of Ramnit-infected computers and allows Defendants to carry out the web-inject attacks. This also makes it nearly impossible for users to detect the attacks.

40. Additionally, Ramnit will search the hard-drive of the infected computer and will steal documents that contain certain file names indicating that they contain either financial information or sensitive credentials. The Ramnit bot then uploads this information to the command and control server for further exploitation by Defendants.

41. Further, Ramnit provides a built-in Virtual Network Console ("VNC") server with the ability to connect out to a remote server. This feature allows Defendants to directly access the infected computer over the Internet, bypassing network address translation and firewall restrictions on inbound connections. From this point, the botnet operator can connect the user's computer to the user's bank, and use the login information previously stolen from the user to empty the user's bank accounts.

42. Additionally, Ramnit can take a series of screenshots of the user's browsing session, allowing Defendants to later reconstruct the browsing session. This feature could be used to steal sensitive information such as account balances, or to acquire authentication information. This knowledge could be valuable to a malicious actor to better understand how an online banking application works.

Injuries Resulting From Defendants' Illegal Conduct

43. The Ramnit malware infection harms Microsoft and Microsoft's customers by damaging the customers' computers and the software installed on their computers licensed from Microsoft. During the infection of a user's computer, the Ramnit malware makes changes at the deepest and most sensitive levels of the computer's operating system. Additionally, it makes fundamental changes at the level of the Windows Registry. Microsoft's customers whose computers are infected with the malicious software are damaged by these changes to Windows, which alter the normal and approved settings and functions of the user's operating system, destabilize it, and forcibly draft the customers' computers into the botnet.

44. Once a computer is infected, the Windows operating system and Internet Explorer browser applications on that computer cease to operate normally and are transformed into tools of deception and theft. But Windows and Internet Explorer still bear Microsoft's trademarks. Customers who experience degraded performance of Microsoft's products may attribute such poor performance to Microsoft, causing extreme damage to Microsoft's brands and trademarks and the goodwill associated therewith. Even customers who eventually come to learn their computers are infected with malware may incorrectly attribute the infection to vulnerabilities in Microsoft's products, because many customers are unaware that they have fallen prey to Defendants' attacks.

45. Moreover, as a provider of the Windows and Internet Explorer products, Microsoft devotes significant computing and human resources to combating infections by the Ramnit Botnet, helping customers determine whether or not their computers are infected, and cleaning infected computers. These efforts by Microsoft cost substantial sums of money, and thus the Ramnit Botnet and malware exact a tangible economic toll on Microsoft.

46. The Ramnit Botnets and malware cause injury to numerous consumers, as well as the financial institutions whose interests are represented by FS-ISAC and FS-ISAC itself. Like Microsoft, FS-ISAC has devoted substantial resources to investigating and remediating the harm caused by the Ramnit botnets. In addition, FS-ISAC institutions have their trademarks, brand names, and trade names misused to deceive owners of Ramnit-infected computers to provide

Defendants their login credentials and other personal identifying information. FS-ISAC institutions, moreover, suffer direct financial harm as a result of Defendants' unlawful conduct. Defendants and the Ramnit botnets have cost FS-ISAC member institutions millions.

**Defendants Work Together In A Common Operation
To Create, Control, Maintain, And Operate The Ramnit Botnets**

47. The Ramnit botnets comprise a family of inter-related botnets—commonly known as the Ramnit malware. The Ramnit malware first emerged in January 2010, and while its purpose was not immediately clear, security researchers determined that it was among the fastest spreading infections on the Internet. The Ramnit malware evolved over time to include additional modules that increase functionality for criminal activity.

48. Plaintiffs are informed and believe and thereupon allege that the common code and characteristics of the infected computers in the Ramnit botnet, and evidence regarding specific activities of Defendants, demonstrate that Defendants—acting in concert with each other—control the Ramnit botnet. Upon information and belief, the Ramnit malware that Defendants install on users' computers all share common code and characteristics. The Ramnit bots use similar configuration files, including configuration files from the Zeus family of botnets. The Ramnit configuration files, moreover, share similar structures and use similar commands to command and to control Ramnit-infected user computers. Defendants, moreover, rely on the same domains, name servers, and IP addresses that comprise the Ramnit Command and Control Infrastructure.

49. Each of the Defendants have participated in the Ramnit enterprise by: (1) generating Ramnit executable files, configuration files, and plug-ins to control user computers; (2) deploying the Ramnit botnets under one botnet name; (3) creating and maintaining the Ramnit Command and Control Infrastructure consisting of server computers connected to the Internet through which to communicate with the infected user computers; (4) using one or more means to cause user computers to become infected with Ramnit; (5) using the Ramnit-infected computers around the world to steal sensitive identification and financial account information; (6) using the Ramnit bots to steal money directly from financial accounts of unsuspecting users

around the world; (7) damaging Microsoft-owned and licensed software, including Windows and Internet Explorer, by corrupting these programs' behavior and converting them to instruments of criminality; and (8) exploiting the famous brands and trademarks of Plaintiffs to mislead their customers or customers of their member organizations, and consequently causing severe harm to Plaintiffs' brands, trademarks, reputation, and goodwill.

50. As set forth in detail herein, Defendants have used the Ramnit botnets to steal, intercept and obtain this access device information from tens of thousands of individuals using falsified web pages, and have then used these fraudulently obtained unauthorized access devices to steal millions of dollars from individuals' accounts.

51. Upon information and belief, Defendants have conspired to, and have, executed a scheme to defraud scores of financial institutions by enabling Defendants to fraudulently represent themselves as specific bank customers, thereby enabling them to access and steal funds from those customer accounts. Defendants have also victimized consumers by stealing monies, data, and by taking control of victim computers without authorization.

FIRST CLAIM FOR RELIEF

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

52. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 51 above.

53. Defendants knowingly and intentionally accessed protected computers without authorization and knowingly caused the transmission of a program, information, code and commands, resulting in damage to the protected computers, the software residing thereon, and Microsoft.

54. Defendants' conduct involved interstate and/or foreign communications.

55. Defendants' conduct has caused a loss to each Plaintiff during a one-year period aggregating at least \$5,000.

56. Plaintiffs seek injunctive relief and 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, Plaintiffs have suffered and continue to

suffer irreparable harm for which there is 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. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 57 above.

59. Microsoft's Windows operating system and Internet Explorer software, and Microsoft's customers' computers running such software, are facilities through which electronic communication service is provided to Microsoft's users and customers.

60. Defendants knowingly and intentionally accessed the Windows operating system and Internet Explorer software and computers upon which it runs without authorization or in excess of any authorization granted by Microsoft or any other party.

61. Through this unauthorized access, Defendants intercepted, had access to, obtained and altered, and/or prevented legitimate, authorized access to, wire electronic communications transmitted via Microsoft's Windows operating system and Internet Explorer software and the computers running such software.

62. Plaintiffs seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

63. As a direct result of Defendants' actions, Plaintiffs have suffered and continue to suffer irreparable harm for which no adequate remedy at law exists, 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.*

64. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 63 above.

65. Defendants have used Microsoft's and FS-ISAC institutions' trademarks in interstate commerce, including Microsoft's federally registered trademarks for the word marks Microsoft®, Windows®, and Internet Explorer® .

66. The Ramnit botnet generates and uses unauthorized copies of Microsoft's trademarks in fake and unauthorized versions of the Windows operating system and Internet Explorer software, including through the software operating from and through the Ramnit Command and Control Infrastructure. The Ramnit botnet also generates and use unauthorized copies of FS-ISAC institutions' trademarks. By doing so, Defendants are likely to cause confusion, mistake, or deception as to the origin, sponsorship, or approval of the fake and unauthorized versions of the Windows operating system and Internet Explorer software.

67. As a result of their wrongful conduct, Defendants are liable to Plaintiffs for violation of the Lanham Act.

68. Plaintiffs seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

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

70. Defendants' wrongful and unauthorized use of Microsoft's and FS-ISAC institutions' trademarks 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)

71. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 70 above.

72. Microsoft's and FS-ISAC member institutions' trademarks are distinctive marks that are associated with Microsoft and FS-ISAC member institutions and exclusively identify their businesses, products, and services.

73. Defendants make unauthorized use of Microsoft's and FS-ISAC member institutions' trademarks. By doing so, Defendants create false designations of origin as to tainted Microsoft products and FS-ISAC member institution services that are likely to cause confusion, mistake, or deception.

74. As a result of their wrongful conduct, Defendants are liable to Plaintiffs for violation of the Lanham Act, 15 U.S.C. § 1125(a).

75. Plaintiffs seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

76. As a direct result of Defendants' actions, Plaintiffs have suffered and continue to suffer irreparable harm for which they have 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)

77. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 76 above.

78. Microsoft's and FS-ISAC member institutions' trademarks are famous marks that are associated with Microsoft and FS-ISAC member institutions and exclusively identify their businesses, products, and services.

79. Defendants make unauthorized use of Microsoft's and FS-ISAC member institutions' trademarks. By doing so, Defendants are likely to cause dilution by tarnishment of Plaintiffs' trademarks.

80. Plaintiffs seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

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

SIXTH CLAIM FOR RELIEF

Common Law Trespass to Chattels

82. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 81 above.

83. Defendants have used a computer and/or computer network, without authority, with the intent to cause physical injury to the property of another.

84. Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to trespass on the computers and computer networks of FS-ISAC member institutions.

85. Defendants' actions in operating the Ramnit Botnet result in unauthorized access to Microsoft's Windows operating system and Internet Explorer software and the computers on which such programs run, and result in unauthorized intrusion into those computers and theft of information, account credentials, and funds.

86. Defendants intentionally caused this conduct and this conduct was unlawful and unauthorized.

87. Defendants' actions have caused injury to Microsoft, FS-ISAC, and FS-ISAC member institutions, and have interfered with the possessory interests of Microsoft over its software and with the FS-ISAC member institutions' possessory interests in their respective computers and computer networks.

88. Plaintiffs seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

89. As a direct result of Defendants' actions, Plaintiffs and FS-ISAC member institutions have suffered and continue to suffer irreparable harm for which no adequate remedy at law exists, and which will continue unless Defendants' actions are enjoined.

SEVENTH CLAIM FOR RELIEF

Unjust Enrichment

90. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 89 above.

91. The acts of Defendants complained of herein constitute unjust enrichment of the Defendants at the expense of Microsoft and FS-ISAC member institutions in violation of the common law. Defendants used, without authorization or license, software belonging to Microsoft to facilitate unlawful conduct inuring to the benefit of Defendants.

92. Defendants profited unjustly from their unauthorized and unlicensed use of Microsoft's intellectual property.

93. Upon information and belief, Defendants had an appreciation and knowledge of the benefit they derived from their unauthorized and unlicensed use of Microsoft's intellectual property.

94. Retention by the Defendants of the profits they derived from their malfeasance would be inequitable.

95. Plaintiffs seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial, including without limitation disgorgement of Defendants' ill-gotten profits.

96. As a direct result of Defendants' actions, Plaintiffs and FS-ISAC member institutions suffered and continue to suffer irreparable harm for which no adequate remedy at law exists, and which will continue unless Defendants' actions are enjoined.

EIGHTH CLAIM FOR RELIEF

Conversion

97. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 96 above.

98. Microsoft owns all right, title, and interest in its Windows and Internet Explorer software. Microsoft licenses its software to end-users. Defendants have interfered with, unlawfully and without authorization, and dispossessed Microsoft of control over its Windows and Internet Explorer software.

99. Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to remove, halt, or otherwise disable computer data, computer programs, and computer software from a computer or computer network.

100. Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to cause a computer to malfunction.

101. Defendants have converted funds from FS-ISAC member institutions through unauthorized withdrawals of funds from customer accounts using stolen online banking credentials.

102. Plaintiffs seek injunctive relief and compensatory and punitive damages in an

amount to be proven at trial, including without limitation the return of Defendants' ill-gotten profits.

103. As a direct result of Defendants' actions, Plaintiffs and FS-ISAC member institutions suffered and continue to suffer irreparable harm for which no adequate remedy at law exists, and which will continue unless Defendants' actions are enjoined.

NINTH CLAIM FOR RELIEF

Intentional Interference with Contractual Relationships

104. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 103 above.

105. Microsoft has valid and subsisting contractual relationships with licensees of its Windows and Internet Explorer products. Microsoft's contracts confer economic benefit on Microsoft.

106. Defendants' conduct interferes with Microsoft's contractual relationships by impairing, and in some instances destroying, the products and services Microsoft provides to its customers. On information and belief, Defendants know that their conduct is likely to interfere with Microsoft's contracts and to deprive Microsoft of the attendant economic benefits.

107. On information and belief, Microsoft has lost licensees due to Defendants' conduct.

108. Defendants' conduct has caused Microsoft economic harm. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs prays that the Court:

1. Enter judgment in favor of Plaintiffs 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 domains used by Defendants to cause injury and enjoining Defendants from using such instrumentalities.
5. Enter judgment awarding Plaintiffs actual damages from Defendants adequate to compensate Plaintiffs 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: February 19, 2015

Respectfully submitted,

ORRICK, HERRINGTON & SUTCLIFFE
LLP



DAVID B. SMITH
Va. State Bar No. 84462
Attorneys for Plaintiffs Microsoft Corp. and FS-ISAC, Inc.
ORRICK, HERRINGTON & SUTCLIFFE LLP
Columbia Center
1152 15th Street, N.W.
Washington, D.C. 20005-1706
Telephone: (202) 339-8400
Facsimile: (202) 339-8500
dsmith@orrick.com

Of counsel:

GABRIEL M. RAMSEY (*pro hac vice* application pending)
JACOB M. HEATH (*pro hac vice* application pending)
ROBERT L. URIARTE (*pro hac vice* application pending)
Attorneys for Microsoft Corp. and FS-ISAC, Inc.
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
ruriarte@orrick.com

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

RICHARD DOMINGUES BOSCOVICH (*pro hac vice*
application pending)
MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052-6399
Telephone: (425) 704-0867
Facsimile: (425) 936-7329
rbosco@microsoft.com

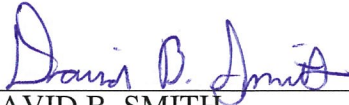
DEMAND FOR JURY TRIAL

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

Dated: February 20, 2015

Respectfully submitted,

ORRICK, HERRINGTON & SUTCLIFFE
LLP



DAVID B. SMITH
Va. State Bar No. 84462
Attorneys for Plaintiffs Microsoft Corp. and FS-ISAC, Inc.
ORRICK, HERRINGTON & SUTCLIFFE LLP
Columbia Center
1152 15th Street, N.W.
Washington, D.C. 20005-1706
Telephone: (202) 339-8400
Facsimile: (202) 339-8500
dsmith@orrick.com

Of counsel:

GABRIEL M. RAMSEY (*pro hac vice* application pending)
JACOB M. HEATH (*pro hac vice* application pending)
ROBERT L. URIARTE (*pro hac vice* application pending)
Attorneys for Microsoft Corp. and FS-ISAC, Inc.
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
ruriarte@orrick.com

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

RICHARD DOMINGUES BOSCOVICH (*pro hac vice*
application pending)
MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052-6399
Telephone: (425) 704-0867
Facsimile: (425) 936-7329
rbosco@microsoft.com

APPENDIX A

REGISTRY FOR .COM DOMAINS

Verisign Naming Services
21345 Ridgetop Circle
4th Floor
Dulles, Virginia 20166
United States

Verisign Global Registry Services
12061 Bluemont Way
Reston Virginia 20190
United States

CURRENTLY REGISTERED .COM DOMAINS

anxsmqyfy.com
campbrusderapp.com
jhghrlufoh.com
khllpmpmare.com
knpqxlxcwtlvgrdyhd.com
nvlyffua.com
ppyblaohb.com
riaaiysk.com
santabellasedra.com
tqjhvyhf.com
vrndmdrdrjoff.com

DEFENDANTS JOHN DOES 1 – 3 CONTACT INFORMATION

caewoodydr@uymail.com
campmorgenapp@arcticmail.com
carmiller@mail.com
redswoodster@engineer.com
gromsmoothe@arcticmail.com

UNREGISTERED .COM BACKUP DOMAINS GENERATED BY BOTNET

| | |
|-------------------------|-------------------------|
| acuhjbadvnmhthwnlxv.com | ayketyjlsaeu.com |
| advvpbrtyw.com | bltolwbwychlyt.com |
| aflgqgddfi.com | bmaucdrfpmnh.com |
| apbhwiohxqbvoxlumdh.com | bmjjksysowdwmoy.com |
| apkdwbwdpickk.com | bmjvrxrqpkwdrdv.com |
| aprocqhqmml.com | bpiwebgqddyvgcnjgh.com |
| asldoqoolcgm.com | briujbxmkjeusvslrn.com |
| aufdloglxlqoxlepp.com | bseboouatanfddgbrdv.com |
| avxvatwmxwbyiepwmo.com | bvqdvfiwnaja.com |

cbxyvrxewvlnxhkadfg.com
ccylbclg.com
cgwootylkoyxe.com
cjagpjgd.com
ckgvnbwdywbxvlnk.com
clkcdjjmyylwib.com
cqvyephudwsuqjhge.com
croxxnrtvrqt.com
cuhbjlgw.com
cyanlvwkuatvmw.com
dbygksqtu.com
dfalxqubjhl.com
dfvxuvljbykia.com
dhfejwhoj.com
dledwgrxiispx.com
dnqjposxrelhqqplwli.com
duhjquituiokycypi.com
dwbdecmppklvbevvtjq.com
dwksmbrq.com
dxktegertgbgeoi.com
dxzteubknwecsduftp.com
ealxbraobohxb.com
ebrfoys.com
ecsgmpariu.com
edvxemrsvvycwt.com
egopuefrdsefc.com
eipvatwwexl.com
ejfrcfwdbsaahdt.com
emlxeyirx.com
emxwjwddb.com
ersbvvdxdamjotwpm.com
etjdsnpjvb.com
euvyalbkwahxxjn.com
evrlsscrxvmd.com
exmfhgyv.com
eyvvpstmcwwwvsyjtif.com
facmttijcdq.com
fgcdhqgcedomle.com
fjdmkqvralmgorinlc.com
fkcfkeygpldjer.com
fndjnmskmjhjq.com
finjboahxkasxdl.com
fmqegimr.com
fsxgfwychumgrgmhwo.com
fuogcmhewqer.com
fvkcrcflhy.com

fxngienbgebck.com
fycecyuksgjfx.com
gaqqerty.com
gbcpynphvropsyu.com
gdekatkjjihi.com
gmsxrgagrfgivh.com
gqnoupteuivrwte.com
grbfnxxej.com
gtiswnukb.com
guifymdmxj.com
gunqwxgyrl.com
gwmjxjueqme.com
gwnppapgwhtidegx.com
hajqfvvqjkkajewi.com
hjahmdueyebf.com
hjvlshecwshpfxwfl.com
hllcololi.com
hllnakmxmgoyh.com
hlrsxjdakvl.com
hoeqosqeicddv.com
hqskceeltysbbnc.com
hvkxvhkmfsdgd.com
hvyfjjqdlwhnlrpaa.com
hwruijnk.com
ibvtknxochoyjidm.com
icqkxusbfdwhy.com
ifbomanec.com
ijfwbyvcirepgd.com
ikkjjgbqgts.com
ilpvrpxwfauqaxyq.com
imvfakaudq.com
iqhafgpvsrj.com
ixwnsfmyg.com
iylelocfsj.com
jherkljcsloepd.com
jhfykbugthmdkgga.com
jhrqfnrlpyvo.com
jjdvasey.com
jkgvbneenmrbklortr.com
jkyolccxfy.com
jmesrbwtcejev.com
jmmurxyktxvegxsid.com
jnjjlojgnvxesr.com
jvmckcospyqedcsjny.com
jycxmcdof.com
jymqfxgwfhyms.com

kavkwpjdndsk.com
kcilhmepervm.com
kdjsnsre.com
kdkdpwql.com
kjpsjoxqsutgewlrah.com
kuwkdqstblavept.com
kvcovjrpsb.com
kvfkfxakmqoof.com
kynknfyngikfno.com
kyskhoopsmkbmenau.com
labxpyvjtuijwghie.com
lcqavndroo.com
lehmgspxp.com
liedjckipkehqxwtdl.com
llgnygbqh.v.com
llurxdkpkbvjx.com
lorwmtrf.com
lpivbutq.com
lpvdauemfexnvoyh.com
lsvnoumbqcsjl.com
ltrpfybf.com
luvrqdhavhxcbtc.com
lvqdhqrhfxlsglkf.com
lvrjjmbdtfapwev.com
lwnngpwijlvayagmu.com
lybfxrtdkdbbqr.com
lyftposyknpigp.com
lyvxrtpkchmddb.com
lyxbotuappfreadkfk.com
mbpnjenhxgcimx.com
mchpmdywg.s.com
mfnaqngqorgbxbnsc.com
mhuvivlyndmsx.com
mioqhqvmduqicvoey.com
mkdnthiyqlq.com
mktxegrucbkv.com
mlgdwljfmnkt.com
mqojcxmnnxy.com
muabyljiutasgqedl.com
mxgainbmtvariv.com
myhyfpuoh.com
myqenkelfk.com
nbkqygsfvri.com
nfbodxdevgpjba.com
nfqhufvxyssyda.com
nglqogrh.com

nhcdrnwpsasnaar.com
nqgsmbkwnifdyost.com
nqnyteqxqgqohvco.com
ntikqcjtehpih.com
nvgmdyabspq.com
nwuqfobauwsyuppii.com
nxhdmugxeiht.com
nxxuwtws.com
ocvqccdenkjs.com
odcenmfimwibhrfvvxy.com
oexdjxjdoiplmxfybbm.com
ogfavvwxus.com
ogmwrgrgk.com
okfatclblpl.com
ootuuujaep.com
optiidevdabtlewjd.com
otdvlbjeucwyqkfbn.com
ovhlfqcpfxyjgjb.com
ovtindng.com
ovypjimjcnvwooiamj.com
owerubvhcinavarinm.com
oyuqibrjowbfmvj.com
oyxmxbsppuucbtwm.com
pacffcnx.com
pbdlsfkjrxclqjo.com
pgnpuktvbnmrybjsv.com
pgtuyjyovgffyfrn.com
pnfnkahiodseewyen.com
ppvrnfkbarbnlm.com
ptvaolhg.com
pxjjwmhlmpbtsvhuq.com
qdboaveuhwabhwik.com
qglhlsyskvufb.com
qhnhlgmfepeulxtpkv.com
qiisbgyqkrokowrbq.com
qnnyirhtuautt.com
qpfvbstn.com
qyvbditfgmkxqjrik.com
qvberjspofqsxdnr.com
qwmqyrcvkseynvrgdnv.com
qxqkdvwayhengjqm.com
qyuylvjwh.com
repliinqssbrnf.com
rgrtvwsmalhm.x.com
rijfxtotkuysyfh.com

5
rjbejalpcsgghdm.com
rmdmqetbpbpgpufhql.com
rmjkunxkbcrslfbc.com
rrewytfucjjylju.com
rwcdljyemxplouufjvd.com
sblbtuqtiavvtrkrn.com
sbpvpkuwoxevjy.com
scfxvdlmfbgf.com
sdjvmbngpgwnpdj.com
shnlojyteeoctymxe.com
slvmktdpxdd.com
smisifkrfkyccnlk.com
snpryjitnos.com
srjkrxvxmkuql.com
srvmkdeaerccaffs.com
ssclrhiimfeodm.com
sthspflawbhacxp.com
tbajypaiecloxihf.com
tjslktadjklb.com
tnqtdfodepctna.com
todyennhm.com
twwrktawwgpito.com
typmyloijdcxtdxd.com
ucfenxbryboqwbmlxke.com
udiivoyrbugyfruq.com
uehhvrdnuc.com
ugkrxtjrlfbxmakmt.com
uoidxmhugvidc.com
upnsdndflqokigybdrr.com
uuofllccd.com
uvkejdriqublsst.com
vcssgidqhkar.com
vdbtvdpujtfhwa.com
vefqierysov.com
veymlvyoknk.com
vffamysgfsodw.com
vfrpojablslkqr.com
vilapacdnnodhsehneh.com
vlglwuyqoxjn.com
vpwxxqwcndrxpc.com
vrvfonqdkfjo.com
vwlcnujosuovul.com
wacwpqx.com
wehtwbqu.com
wgvmlfygce.com
wjpsxawqxomokepfbw.com

wknfjeopkdj.com
wldlrwlygck.com
wnftxxhnwiugtvywo.com
wvmmvpbkjrd.com
wxkeojjdshd.com
wxxnufbeacmrtam.com
xbjersli.com
xcpvexsyqsf.com
xdtfqohfbskcgxameg.com
xdyowsheht.com
xirrlpllrcofqs.com
xktepjakoyq.com
xlqaburwns.com
xmlonthptunynnxf.com
xnttexmtc.com
xoqxabqb.com
xrtgqevawtlmulghj.com
xsmypdmnacrqxkdb.com
xtbwxayxxvqspo.com
xuajockq.com
ybgpdikdudmdfr.com
ycafyovxdnlsa.com
ycmusvulvknobnbwhvp.com
yctgocejemh.com
yctkhjksne.com
ycvmwjae.com
ydgadpgvne.com
yembvgbgmdipfwjmd.com
yovkoaxsana.com
yoxbjnpkkmkjrj.com
yxibnav.com
yxkhvhehtjfoqrnedi.com
yytbonkxjwy.com

APPENDIX B



United States Patent and Trademark Office

[Home](#) | [Site Index](#) | [Search](#) | [FAQ](#) | [Glossary](#) | [Guides](#) | [Contacts](#) | [eBusiness](#) | [eBiz alerts](#) | [News](#) | [Help](#)

Trademarks > Trademark Electronic Search System (TESS)

TESS was last updated on Fri Nov 22 03:20:26 EST 2013

[TESS HOME](#) [NEW USER](#) [STRUCTURED](#) [FREE FORM](#) [BROWSE LIST](#) [SEARCH OG](#) [BOTTOM](#) [HELP](#)[Logout](#)

Please logout when you are done to release system resources allocated for you.

Record 1 out of 1

[TSDR](#) [ASSIGN Status](#) [TTAB Status](#) (Use the "Back" button of the Internet Browser to return to TESS)

Typed Drawing

| | |
|--------------------------|--|
| Word Mark | MICROSOFT |
| Goods and Services | IC 037. US 100 103 106. G & S: Installation, maintenance and repair of computer networks and computer systems consisting of software. FIRST USE: 19870105. FIRST USE IN COMMERCE: 19870105 |
| Mark Drawing Code | (1) TYPED DRAWING |
| Serial Number | 78190864 |
| Filing Date | December 3, 2002 |
| Current Basis | 1A |
| Original Filing Basis | 1B |
| Published for Opposition | August 5, 2003 |
| Registration Number | 2872708 |
| Registration Date | August 10, 2004 |
| Owner | (REGISTRANT) Microsoft Corporation CORPORATION WASHINGTON One Microsoft Way Redmond WASHINGTON 980526399 |
| Attorney of Record | William O. Ferron, Jr. |
| Prior Registrations | 1200236;1256083;1259874 |
| Type of Mark | SERVICE MARK |
| Register | PRINCIPAL |
| Affidavit Text | SECT 15. SECT 8 (6-YR). |
| Live/Dead Indicator | LIVE |

[TESS HOME](#) [NEW USER](#) [STRUCTURED](#) [FREE FORM](#) [BROWSE LIST](#) [SEARCH OG](#) [TOP](#) [HELP](#)

[HOME](#) | [SITE INDEX](#) | [SEARCH](#) | [eBUSINESS](#) | [HELP](#) | [PRIVACY POLICY](#)



United States Patent and Trademark Office

[Home](#) | [Site Index](#) | [Search](#) | [FAQ](#) | [Glossary](#) | [Guides](#) | [Contacts](#) | [eBusiness](#) | [eBiz alerts](#) | [News](#) | [Help](#)

Trademarks > Trademark Electronic Search System (TESS)

TESS was last updated on Fri Nov 22 03:20:26 EST 2013

[TESS HOME](#) [NEW USER](#) [STRUCTURED](#) [FREE FORM](#) [Browse by Class](#) [SEARCH-OG](#) [BOTTOM](#) [HELP](#)[Logout](#)

Please logout when you are done to release system resources allocated for you.

Record 1 out of 1

[TSDR](#)[ASSIGN Status](#)[TTAB Status](#)

(Use the "Back" button of the Internet Browser to return to TESS)

Typed Drawing

| | |
|--------------------------|--|
| Word Mark | WINDOWS |
| Goods and Services | IC 041. US 100 101 107. G & S: providing information over computer networks and global communication networks in the fields of entertainment, music, and interactive games; education services, namely on-line tutorials in the field of computers and computer software. FIRST USE: 19980126. FIRST USE IN COMMERCE: 19980126 |
| Mark Drawing Code | (1) TYPED DRAWING |
| Serial Number | 75879977 |
| Filing Date | December 22, 1999 |
| Current Basis | 1A |
| Original Filing Basis | 1A |
| Published for Opposition | April 3, 2001 |
| Registration Number | 2463526 |
| Registration Date | June 26, 2001 |
| Owner | (REGISTRANT) Microsoft Corporation CORPORATION WASHINGTON One Microsoft Way Redmond WASHINGTON 98052 |
| Attorney of Record | William O. Ferron, Jr. |
| Prior Registrations | 1872264;1875069;1989386;2005901;2212784 |
| Type of Mark | SERVICE MARK |
| Register | PRINCIPAL-2(F) |
| Affidavit Text | SECT 15. SECT 8 (6-YR). SECTION 8(10-YR) 20110311. |
| Renewal | 1ST RENEWAL 20110311 |
| Live/Dead Indicator | LIVE |

[TESS HOME](#) [NEW USER](#) [STRUCTURED](#) [FREE FORM](#) [BROWSE DATA](#) [SEARCH LOG](#) [TSP](#) [HELP](#)

[| HOME](#) [| SITE INDEX](#) [| SEARCH](#) [| eBUSINESS](#) [| HELP](#) [| PRIVACY POLICY](#)



United States Patent and Trademark Office

[Home](#) | [Site Index](#) | [Search](#) | [FAQ](#) | [Glossary](#) | [Guides](#) | [Contacts](#) | [eBusiness](#) | [eBiz alerts](#) | [News](#) | [Help](#)

Trademarks > Trademark Electronic Search System (TESS)

TESS was last updated on Fri Nov 22 03:20:26 EST 2013

[TESS HOME](#)
[NEW USER](#)
[STRUCTURED](#)
[FREE FORM](#)
[Browse Data](#)
[SEARCH OG](#)
[BOTTOM](#)
[HELP](#)

[Logout](#)

Please logout when you are done to release system resources allocated for you.

Record 1 out of 1

[TSDR](#)
[ASSIGN Status](#)
[TTAB Status](#)
 (Use the "Back" button of the Internet Browser to return to TESS)

Typed Drawing

| | |
|--|--|
| Word Mark | INTERNET EXPLORER |
| Goods and Services | IC 009. US 021 023 026 036 038. G & S: browsers, namely, software for browsing the global computer network and secure private networks, and software programs to connect computers to the global computer network and to secure private networks. FIRST USE: 19941000. FIRST USE IN COMMERCE: 19950101 |
| Mark Drawing Code | (1) TYPED DRAWING |
| Serial Number | 75340051 |
| Filing Date | August 13, 1997 |
| Current Basis | 1A |
| Original Filing Basis | 1A |
| Published for Opposition | June 30, 1998 |
| Registration Number | 2277112 |
| International Registration Number | 0861311 |
| Registration Date | September 14, 1999 |
| Owner | (REGISTRANT) SyNet, Inc. CORPORATION ILLINOIS 2148 Oxnard Drive Downers Grove ILLINOIS 60516 |
| | (LAST LISTED OWNER) MICROSOFT CORPORATION CORPORATION WASHINGTON ONE MICROSOFT WAY REDMOND WASHINGTON 980526399 |
| Assignment Recorded | ASSIGNMENT RECORDED |
| Attorney of Record | WILLIAM O. FERRON, JR. |
| Disclaimer | NO CLAIM IS MADE TO THE EXCLUSIVE RIGHT TO USE "INTERNET" APART FROM THE MARK AS SHOWN |
| Type of Mark | TRADEMARK |

| | |
|---------------------|--|
| Register | PRINCIPAL |
| Affidavit Text | SECT 15. SECT 8 (6-YR). SECTION 8(10-YR) 20090314. |
| Renewal | 1ST RENEWAL 20090314 |
| Live/Dead Indicator | LIVE |

| | | | | | | | |
|---------------------------|--------------------------|----------------------------|---------------------------|-----------------------------|---------------------------|---------------------|----------------------|
| TESS HOME | NEW USER | STRUCTURED | FREE FORM | BROWSE LIST | SEARCH OG | TOP | HELP |
|---------------------------|--------------------------|----------------------------|---------------------------|-----------------------------|---------------------------|---------------------|----------------------|

[| HOME](#) | [SITE INDEX](#) | [SEARCH](#) | [eBUSINESS](#) | [HELP](#) | [PRIVACY POLICY](#)