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

MICROSOFT CORPORATION, a Washington Corporation, Plaintiff v. JOHN DOES 1-8 CONTROLLING A COMPUTER BOTNET THEREBY INJURING MICROSOFT AND ITS CUSTOMERS, Defendant.	§ § § § § § § § § § § § §	CASE NO. A13CV1014 **FILED UNDER SEAL**

DECLARATION OF JASON LYONS IN SUPPORT OF APPLICATION OF MICROSOFT CORPORATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER, AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Jason Lyons, declare as follows:

1. I am a Senior Manager in the Digital Crimes Unit of Microsoft Corp.'s ("Microsoft) Legal and Corporate Affairs group. I make this declaration in support of Microsoft's Application For An Emergency Temporary Restraining Order And Order To Show Cause Re Preliminary Injunction ("TRO Application"). I make this declaration of my own personal knowledge. If called as a witness, I could and would testify competently to the truth of the matters set forth herein.

2. In my role at Microsoft, I assess technological security threats to Microsoft and the impact of such threats on Microsoft's business and customers. Among my responsibilities are protecting Microsoft online service assets from network-based attacks. Before joining Microsoft, I worked for Xerox as the Manager of Xerox's Cyber Intelligence Response Team. I also worked for Affiliated Computer Services ("ACS") prior to Xerox's acquisition of ACS. While at ACS, I provided in-court testimony in connection with a temporary restraining order

application concerning misappropriation of ACS's intellectual property. Prior to entering the private sector, I obtained certifications in counterintelligence, digital forensics, computer crime investigations, and digital media collection from the United States Department of Defense. From 1998 to 2005, I served as a Counterintelligence Special Agent in the United States Army. My duties as a Counterintelligence Special Agent included investigating and combating cyber-attacks against the United States.

3. I have read and agree with the declaration of my colleague David Anselmi in support of Microsoft's TRO Application. Mr. Anselmi and I have worked closely together regarding the subject matter of the TRO Application. In this declaration, I will explain the steps that Microsoft anticipates will neutralize the "click fraud" and "browser hijacking" modules of the ZeroAccess botnet.

A. Overview Of A Computer Botnet

4. A "botnet" is a group of compromised (*i.e.*,"hacked") computers that malicious actors or organizations control without the user's knowledge or consent. Botnets consists of hundreds, thousands, or as in the case of the ZeroAccess botnet, millions of infected computers owned by individuals and business. Botnets are grown by infecting computers with malicious software ("malware"). Through this malware, botnet operators remotely control infected computers.

5. To facilitate remote control of a botnet, botnet operators implement a command and control infrastructure whereby they issue instructions to infected computers. These instructions are typically hosted at specialized computers connected to the Internet known as "command and control" servers. Through these command and control servers, cybercriminals coordinate the infected computers, having them engage in illegal conduct, including online advertising fraud.

B. The ZeroAccess Botnet Coordinates Illegal Activity Among Infected Computers

6. I have participated in Microsoft's investigation of the ZeroAccess malware and the ZeroAccess botnets. The ZeroAccess botnet engages in a variety of illegal conduct relating to online advertising fraud, including "click fraud" and "browser hijacking" (concepts explained in detail in the declaration of David Anselmi). The perpetrators of the ZeroAccess botnet have developed distinct modules of malware designed to carry out the various objectives of the botnet (*i.e.*, a click fraud module, a browser hijacking module, a bitcoin mining module, etc.), and they frequently update and refine these distinct pieces of malware in furtherance of their unlawful scheme. Based on Microsoft's investigation, there are currently in excess of 800,000 ZeroAccess-infected computers active on the Internet on any given day. Microsoft estimates that there have been well over 2 million computers afflicted by the ZeroAccess botnet since its inception, and a prominent security researcher recently published a report which concluded that, as of October 2013, there were 1.9 million ZeroAccess-infected computers.

7. The ZeroAccess botnets' operators have structured the botnet in a "Peer-to-Peer" topology. Through its Peer-to-Peer topology, ZeroAccess-infected computers (called "bots" or "nodes") continually communicate with each other in order to maintain and grow the botnet and carry out the botnets' daily functions. This Peer-to-Peer topology allows the cybercriminals behind the ZeroAccess botnet to remotely control the botnet from tens of thousands of different computers.

8. Once the ZeroAccess malware has successfully infected a new computer, the malware instructs the newly-infected computer to search for and contact other active "peer nodes" in order to download the most recently updated set of configuration files and malware modules. Among these downloads are files that effectively contain 18 Internet Protocol (IP) addresses which correspond to specialized servers ("Fraud Control Servers") used to control the

botnet's click fraud and browser hijacking functions.[1] In the remainder of this Declaration, I refer to these 18 IP addresses as the "Fraud Control IP Addresses."

9. I have investigated each of the 18 Fraud Control IP Addresses. Based on publically available "WHOIS" records, the botnet operators use Internet hosting companies in Germany, the Netherlands, Switzerland, Latvia, and Luxembourg to maintain the 18 Fraud Control IP Addresses.

10. The Fraud Control IP Addresses are integral to the ZeroAccess click fraud and browser hijacking operations. When a ZeroAccess click fraud or malware module begins to run on an infected computer, the malware module instructs the infected computer to contact Fraud Control Servers located at the Fraud Control IP Addresses for instructions. For example, when a ZeroAccess-infected computer engages in browser hijacking, it sends a request to a Fraud Control IP Address dedicated to browser hijacking for instructions on what URL the infected computer should be redirected to. A browser-hijacking server located at the Fraud Control IP Address instructs the infected computer where to go. Throughout the life of the botnet, ZeroAccess malware will instruct infected computers to contact one or more of the 18 Fraud Control IP Addresses in order to perform the botnet's illegal activities.

11. The authors of ZeroAccess have demonstrated the ability to adapt the botnet by updating configuration files, revising the ZeroAccess malware to react to countermeasures, and shifting the location of control infrastructure—such as the Fraud Control IP Addresses. If the authors of ZeroAccess change the Fraud Control IP Addresses before the relief requested in the TRO Application is put into effect, the strategy Microsoft has developed to disrupt the click fraud and browser hijacking functions of ZeroAccess will be rendered ineffective for reasons explained below. To understand how the relief requested in the TRO Application will neutralize the click fraud and browser hijacking modules of the ZeroAccess botnet, some background regarding how computers send and receive information on the Internet is required.

---

[1] An IP address is a numerical code associated with a network location where one or more computers connect to the Internet.

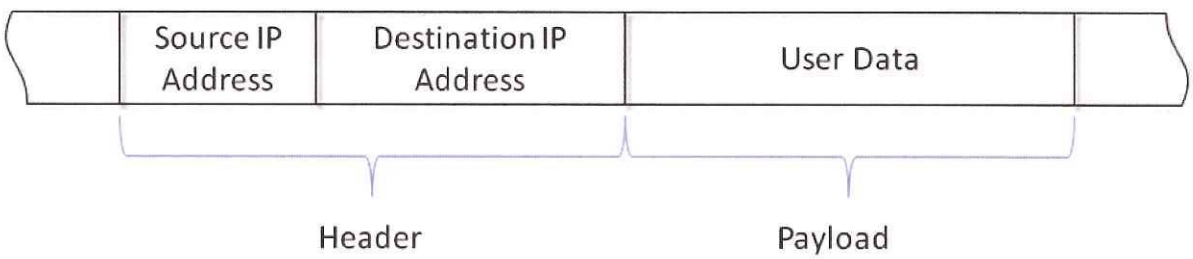
C. Computers Use Internet Service Providers ("ISPs") To Communicate On the Internet

12. The Internet is organized in a hierarchy of computer networks. Internet Service Providers (ISP) provide the physical infrastructure (the "network") necessary to route Internet communications between computers using numerical codes known as IP addresses, which represent locations where one or more computers connect to the Internet.

13. Protocols – *i.e.,* rules and standards – dictate the format of communication over the Internet. Internet protocol requires that users transmit information in "network packets." These packets contain (1) a "header" and (2) user data or "payload." The packet's header contains the data necessary to transmit the payload on the Internet. The header includes the *source IP address* of the computer where the packet originated and the *destination IP address* for the computer that is to receive the packet. **Figure 1** below represents a network packet, the information included in such packets, and where in that packet one would find the source and destination IP addresses.

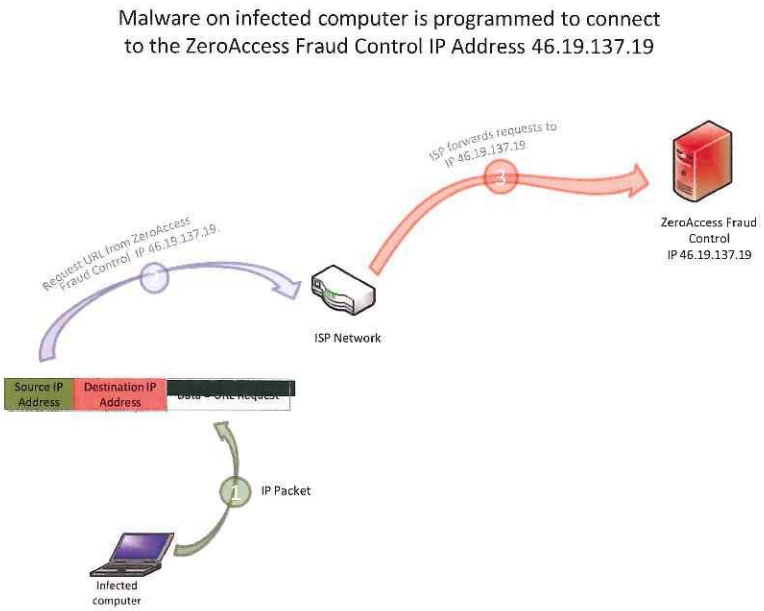
FIGURE 1

IP Packet



14. **Figure 2** illustrates how a ZeroAccess-infected computer will connect to a server ("Fraud Control Server") associated with a Fraud Control IP Address in order to perform browser hijacking. Assume, for example, that ZeroAccess-infected computer has been instructed to contact the Fraud Control IP Address 46.19.137.19 to receive instructions on what URL the infected computer should visit.

FIGURE 2



15. In Step 1, the ZeroAccess-infected computer creates a packet. The packet's header includes the ZeroAccess-infected computer's IP address as the source and the Fraud Control IP Address 46.19.137.19 as the destination.

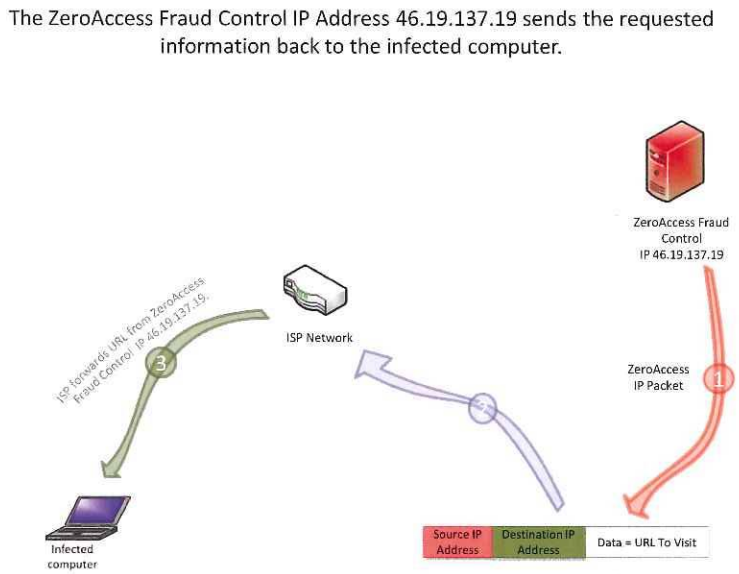
16. In Step 2, the ZeroAccess-infected user computer contacts the ISP and sends the packet to the ISP. Using the destination information in the packet header, the ISP knows where to forward the packet – in this case, a ZeroAccess server located at Fraud Control IP Address 46.19.137.19.

17. In Step 3, knowing the destination of the packet, the ISP forwards the packet to ZeroAccess Fraud Control IP Address, using either its own network or through other networks until that packet reaches the Fraud Control IP Address 46.19.137.19.

18. **Figure 3** explains how a ZeroAccess Fraud Control Server will send information to a ZeroAccess-infected end user. Assume in this example that the ZeroAccess Fraud Control Server, having received a request from a ZeroAccess-infected computer performing browser

hijacking, wants to send a set of instructions telling that computer which URLs to visit. In Step 1, the ZeroAccess Fraud Control Server will construct a packet that contains the IP address 46.19.137.19 for the ZeroAccess Fraud Control Server and the IP address for the destination, the ZeroAccess-infected computer.

FIGURE 3



19. In Step 2, the ZeroAccess Fraud Control Server sends that packet through its hosting provider or ISP network.

20. In Step 3, the ZeroAccess-infected computer's ISP receives the packet. The ISP knows that the packet originated from the IP address 46.19.137.19. The ISP also knows where it should deliver that packet, in this example a ZeroAccess-infected computer. The ZeroAccess-infected computer receives the instructions from the ZeroAccess Fraud Control Server telling the infected computer what URLs to visit.

21. In both examples, the ISP that handles Internet traffic from and to the ZeroAccess-infected computer will have tracked the ZeroAccess Fraud Control IP Address.

D. Effects Of The Court-Ordered Relief

22. I have reviewed the TRO Application and am familiar with the relief Microsoft has requested. Based on the investigation my Microsoft colleagues and I have performed regarding ZeroAccess, I believe the requested relief will disrupt the click fraud and browser hijacking operations of the ZeroAccess botnet.

1. Effects Of Blocking The Fraud Control IP Addresses

23. The most direct means of disrupting the click fraud and browser hijacking operations of the ZeroAccess botnet would be to order the third party hosting companies that maintain the ZeroAccess Fraud Control Servers to sever communication to or from the Fraud Control IP Addresses by preventing those computers from connecting to the Internet. I understand that this Court may not be able to compel such relief because the hosting companies are located outside of the United States.

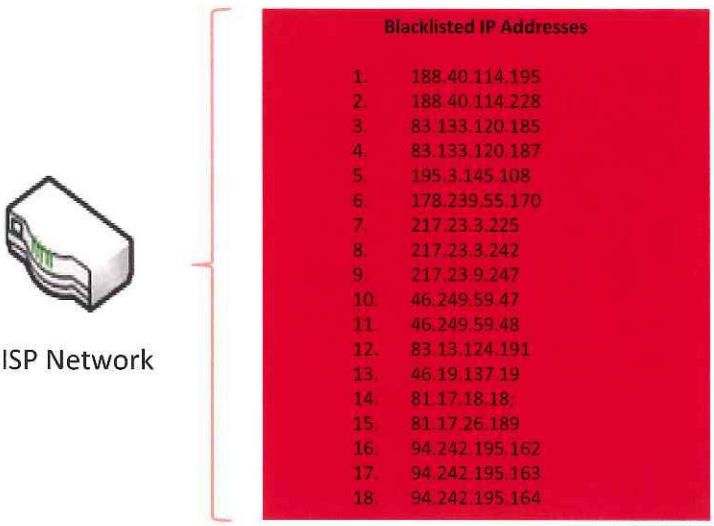
24. Another method of disrupting the click fraud and browser hijacking operations of the ZeroAccess botnet is to order ISPs in the United States to filter traffic to or from the Fraud Control IP Addresses. An ISP handling traffic from and to a ZeroAccess-infected computer tracks the source IP address and the destination IP address of packets transmitted on its networks. As such, it is possible for that ISP to filter Internet traffic to or from a particular IP address. ISPs regularly filter Internet traffic based on "blacklists" – a list of Internet domains or IP addresses known for transmitting unwanted and/or harmful information. Attached hereto as **Exhibit 1** is a true and correct copy of an article entitled "Filtering Sources of Unwanted Traffic Based on Blacklists" authored by individuals from the University of Irvine and AT&T Research. Filtering Internet traffic based on IP addresses is a common ISP practice.

a. ZeroAccess-Infected Computers Will No Longer Communicate With The ZeroAccess Fraud Control Servers

25. If the Court grants Microsoft's requested relief and requires the ISPs to identify and block outgoing and/or incoming Internet traffic on their respective networks to or from a Fraud Control IP Address, communication between ZeroAccess-infected computers and the

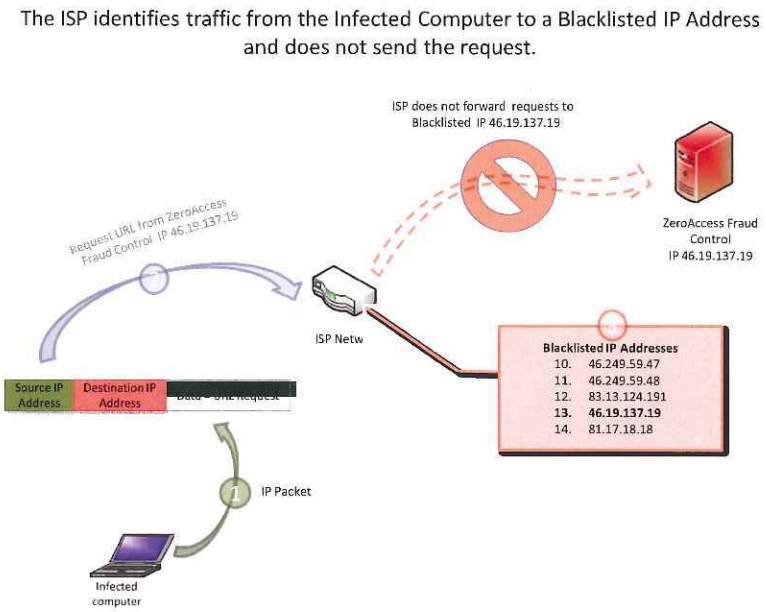
ZeroAccess Fraud Control Servers would cease, disrupting their ability to carry out click fraud and browser hijacking operations. Anytime a packet the ISP identifies a packet containing a Fraud Control IP Address, the ISP would prevent successful delivery of those messages, thereby blocking infected computers from receiving instructions on how to perform click fraud and browser hijacking. **Figure 4** is an example of what a blacklist of the ZeroAccess Fraud IP Addresses would look like.

FIGURE 4



26. **Figure 5** explains the how this relief would block communications from ZeroAccess-infected computers to the Fraud Control Servers. In Step 1, the ZeroAccess-infected computer creates a packet that includes in the header the Fraud Control IP Address 46.19.137.19 as the destination IP address.

FIGURE 5



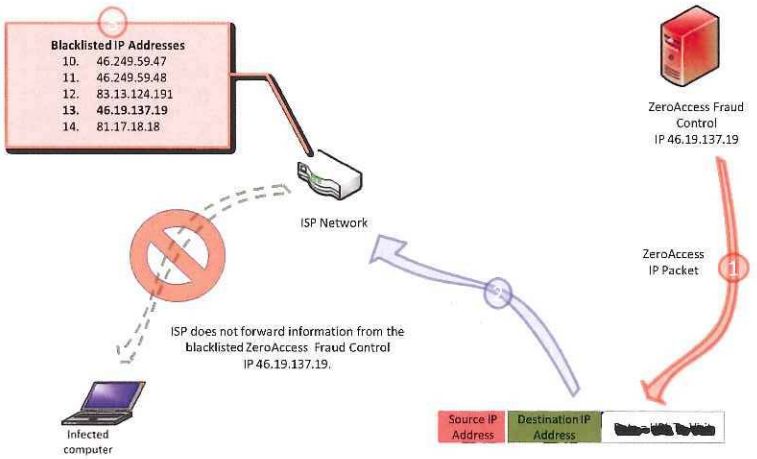
27. In Step 2, the ZeroAccess-infected user computer contacts the ISP and sends the packet to the ISP. Using the destination information in the packet header, the ISP knows where the packet is heading – in this case, a ZeroAccess Fraud Control Server at IP Address 46.19.137.19.

28. In Step 3, recognizing IP address 46.19.137.19 as a blacklisted IP address, the ISP blocks that outbound traffic. The ZeroAccess-infected computer's packet does not reach the Fraud Control Server.

29. **Figure 6** explains how this relief also severs communication from the ZeroAccess Fraud Control Servers to ZeroAccess-infected computers. In Step 1, the ZeroAccess Fraud Control Server will construct a packet that contains the IP address 46.19.137.19 for the ZeroAccess Fraud Control Server as the source IP address.

FIGURE 6

The ISP identifies traffic from the ZeroAccess Fraud Control IP Address and does not send the information back to the Infected Computer.



30. In Step 2, the ZeroAccess Fraud Control Server sends that packet through its hosting provider or ISP network.

31. In Step 3, the ISP servicing the ZeroAccess-infected computer receives the packet. The ISP knows that the packet originated from the IP address 46.19.137.19. Instead of delivering the packet, the ISP filters out the packet. The ZeroAccess-infected computer never receives the information from the ZeroAccess Fraud Control Server.

32. I believe that filtering messages on this level should have no collateral effect on legitimate Internet traffic because only traffic to and from Fraud Control IP Addresses would be filtered. Based on Microsoft's investigation, the only traffic to and from the Fraud Control IP Addresses is traffic generated by the ZeroAccess botnet.

b. Updating The IP "Blacklist" Prevents The Botnet Operators From Reestablishing Contact Between The Fraud Control Servers And Infected Computers

33. When the ZeroAccess botnets' operators notice a substantial number of infected computers are no longer communicating with the Fraud Control Servers, they may push a new

configuration file containing new Fraud Control IP Addresses for new Fraud Control Servers. The ZeroAccess botnet would then rapidly distribute this updated configuration file via the Peer to Peer topology discussed in paragraphs 7 and 8 above.

34. In the event that Defendants move the Fraud Control Servers to new IP addresses, Microsoft will seek that the Court quickly update Appendix A to the TRO to encompass all such new Fraud Control IP addresses that Defendants are shown to use. Updating Appendix A to block any new Fraud Control IP Addresses would prevent the ZeroAccess botnet operators from being able to circumvent the Court's restraining order by relocating the Fraud Control Servers.

2. Blocking Access To The Fraud Control Associated Domain Names

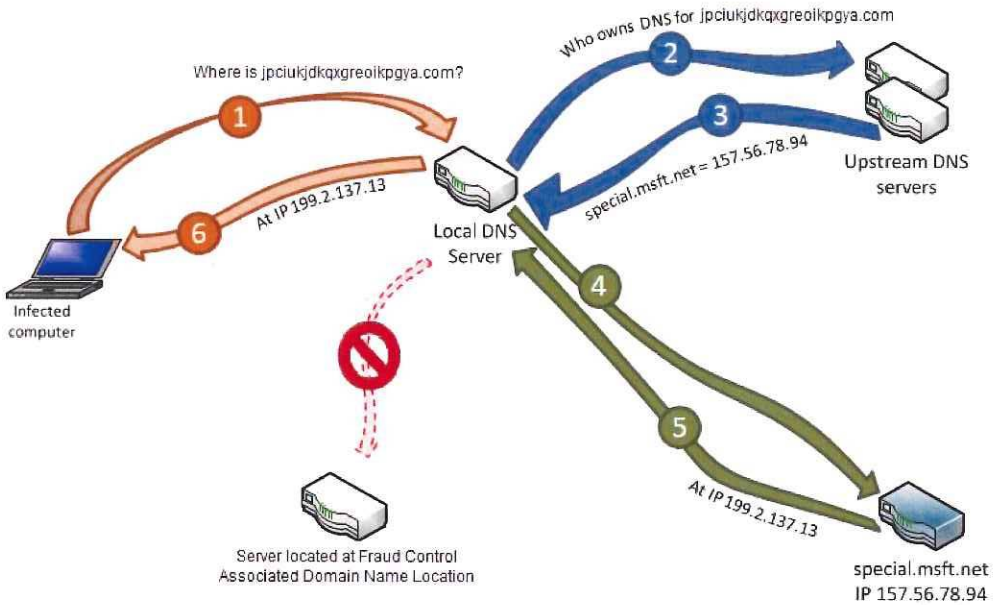
35. Microsoft has discovered that there are 49 domain names embedded in the source code for the click fraud and browser hijacking malware modules. I will refer to these domain names as "Fraud Control Associated Domain Names." The Fraud Control Associated Domain Names have no apparent value or utility, as they consist of seeming random alphanumeric characters that no user would intentionally visit, such as "jpciukjdkqxgreoikpgya.com," "eagdbqufytdxvzbavzriwzgw.com," and "gvkfxhkhbbjoxggsve.com."

36. The purpose of the Fraud Control Associated Domain Names is unclear at present, but Microsoft believes they may be intended to provide fall back control infrastructure for the click fraud and browser hijacking operations in the event that the Fraud Control IP Addresses are blocked. For example, it has been hypothesized by some Microsoft researchers that once the Fraud Control IP Addresses are blocked, the malware modules will direct infected computers to visit the Fraud Control Associated Domain Names to receive instructions. As a precautionary measure against this contingency, Microsoft requests that the Fraud Control Associated Domain names be redirected to Microsoft servers.

37. With respect to the Fraud Control Associated Domain Names, Microsoft's requested relief involves changing the authoritative name servers to servers controlled by Microsoft. Once this occurs, if an infected computer reaches out to a Fraud Control Associated

Domain Name for instructions, it will instead be redirected to a Microsoft server that will display a message to the user that their computer is infected with ZeroAccess. This is depicted in **Figure 7** below.

FIGURE 7



38. In Figure 7, the infected end-user computer attempts to contact the server located at the IP address associated with the Fraud Control Associated Domain Name. In Step 1, the infected computer reaches out to a local Domain Name Server ("DNS") that handles the function of requesting the IP address associated with the domain name from other DNS servers that are higher up in the network hierarchy. In Step 2, The local DNS server queries the upstream DNS server for the IP address of the authoritative name server for that domain name. In Step 3, however, the upstream DNS server has been reconfigured to identify a Microsoft-controlled server, here referred to as "special.msft.net," as the name server. It therefore returns the IP address to special.msft.net to the local DNS server. The user then receives a notice of infection

and is given the opportunity to clean their computer using a program developed by Microsoft, MSERT, that is capable of removing ZeroAccess from the computer.

3. The Curative Steps Microsoft Anticipates Will Promote Disinfection Of ZeroAccess-Infected Computers

39. In the computer security industry, the general model for responding to problems includes four key steps: (1) identification; (2) containment; (3) eradication; and (4) recovery. Here, Microsoft has completed the first of these steps by identifying the ZeroAccess botnet and studying it in detail. The relief requested in the TRO Application would help Microsoft and its industry partners take the second step of containing the harm caused by the ZeroAccess click fraud and browser hijacking operations. In addition, the relief requested in the TRO would facilitate eradication and recovery efforts.

40. As discussed above, the ZeroAccess malware running on an infected computer instructs the computer to communicate with Fraud Control Servers—but the malware also causes an infected computer to communicate with its peer nodes. Although blocking communications between the ZeroAccess Fraud Control Servers and infected computers will stop the botnet's click fraud and browser hijacking operations, ultimately, removing the ZeroAccess malware from the infected computer is required to remove the computer from the ZeroAccess botnet.

41. If the Court grants Microsoft's requested relief, it will facilitate Microsoft's long term eradication and recovery efforts. Microsoft has already developed a tool for removing ZeroAccess malware from infected computers—MSERT—and is working with several ISPs in an effort to provide this tool to their customers. Once the ZeroAccess malware is removed, that computer is no longer part of the botnet and can no longer engage in illegal and harmful conduct. The communication and cooperation between Microsoft and ISPs that will be necessitated by an order granting Microsoft's TRO Application will facilitate Microsoft's efforts to make MSERT available to afflicted users through their ISPs. Moreover, to the extent that the hypothesis discussed above concerning the Fraud Control Associated Domain Names is correct, redirecting

infected computers to a Microsoft server where MSERT is provided will directly facilitate cleaning infected computers.

42. Microsoft believes that the steps discussed in this Declaration provide the best available means of halting the harm caused by the click fraud and browser hijacking operations of the ZeroAccess botnets. Microsoft also believes that obtaining the relief requested in the TRO Application will be an important step towards the ultimate goal of eradicating the ZeroAccess botnet.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed this 24th day of November, 2013 in Austin, Texas.

Jason Lyons