IN THE UNITED STATES DISTRICT COURT

FOR THE WESTERN DISTRICT OF NORTH CAROLINA

CHARLOTTE DIVISION

MICROSOFT CORPORATION, Plaintiff, v. JOHN DOES 1-82, CONTROLLING A COMPUTER BOTNET THEREBY INJURING MICROSOFT AND ITS CUSTOMERS, Defendants.	**FILED UNDER SEAL** Civil Action No. _____ **DECLARATION OF DAVID ANSELMI IN SUPPORT OF MICROSOFT'S APPLICATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER, SEIZURE ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

I, David Anselmi, declare as follows:

1. I am a Senior Manager of Investigations in the Digital Crimes Unit of Microsoft Corp.'s 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. I make this declaration of my own personal knowledge, and, 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. Prior to my current role, I worked as Senior Technologist, dealing with security of Microsoft's online services. Among my responsibilities were protecting Microsoft online service assets from network-based attacks. Prior to that, while also employed by Microsoft, I worked as a Senior Technologist, dealing with protecting

Microsoft's corporate resources from network-based attacks. Before joining Microsoft, I worked for Excell Data Corporation as a Program Manager performing security firewall deployment, configuration, and administration. I am a graduate of the United States Military Academy, West Point, and served for 27 years as a United States Army Communications Electronics Officer (11 years active, 16 reserve), attaining the rank of Lieutenant Colonel.

3. In this declaration, I will explain the steps needed to neutralize and then remove the Citadel malware infecting end-user computers world-wide.

4. The Citadel malware (the Citadel "bots") running on infected end-user computers are programmed to contact one or more domains or IP addresses on the Internet as soon as they successfully infect a new computer. A domain can be thought of as an address on the Internet. Domains are often associated with websites, but they may just be connection points for computers with no website interfaces. An IP address is a numeric code associated with a network location address where one or more computers are connected to the Internet. For ease of reference, in the remainder of this Declaration, I will refer to the Citadel command and control domains and IP addresses communicated with by an infected end-user computer as that computer's "Contact Points." These first Contact Points are "hard-coded" into the bot's executable code, which means that they were put into the bot at the time the bot was created, are an integral part of the bot, and they cannot be changed. After contacting one of these Contact Points, the Citadel bot on the infected personal computer will download additional instructions in the form of an encrypted configuration file that will control the day-to-day operation of the bot.

5. Among other instructions, this configuration file contains a list of additional Citadel Contact Points. When an infected computer is running, the bot will attempt to communicate with at least one of these every twenty minutes for the life of the bot. If it

establishes a connection, it asks the server at the Contact Point whether or not a new configuration file is available. If one is, it downloads it, and disposes of its old configuration file. If its current configuration file is the most recent available, it continues with that. Through this mechanism, the operators of the botnet can control all of the bots running on infected end-user computers.

6. If a Citadel bot cannot establish a connection with the Contact Point it first tries, it works its way down its list of alternative Contact Points, attempting to contact each. If it fails to connect to any of the Contact Points in its configuration file, it reverts to the Contact Points that are hard-coded in the bot executable that was first downloaded in the initial infection. If it fails to connect to any of these, it starts back at the top of the list in its configuration file and iterates through those. It will continue these iterations every twenty minutes until it makes a connection for as long as the bot remains on the user's computer.

A. Computers Use The Domain Name Service ("DNS") To Find Other Computers On The Internet

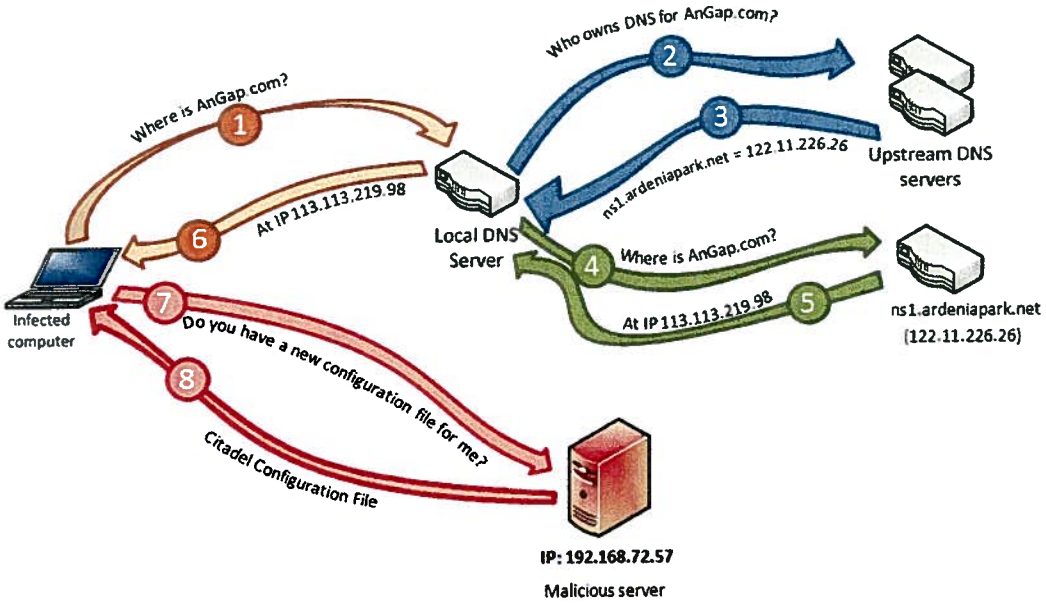
7. To understand how the requested relief in this case will neutralize Citadel botnets, some background in Internet infrastructure may be helpful. Generally, every domain is associated with physical computers, and the place at which a physical computer is connected to the Internet is expressed as the computer's IP address. When a user, or as is the case here, the Citadel bot attempts to contact a domain on the Internet, the process by which it finds the one or more computers associated with that domain is analogous, at a general level, to how a phone book is used. In this analogy, the domain name is analogous to someone's name in the phone book, and the IP address is analogous to the phone number associated with that person's name. On the Internet, the process of connecting a domain name to the IP address of one or more computers supporting that domain is handled by the Domain Name System, or "DNS," which

simply functions as part of the normal infrastructure of the Internet.

8. When a Citadel-infected personal computer seeks to contact its command and control server, it relies on a network of Domain Name Servers, or "DNS servers," that perform the role of keeping track of the IP addresses associated with every domain name on the Internet. A *name server* is a type of DNS server that provides answers to DNS requests for specific domains. If a person wants to connect to a website of a certain name, that person's computer needs to request the IP address of that domain name from a DNS server, which will ultimately submit the request to the name server for that domain. In our phone book analogy, this might be analogous to consulting a separate phone book for businesses or for private individuals, depending on what you wanted to find. This process will be explained with reference to Figure 1, below.

Figure 1

Malware on infected system is programmed to connect to "AnGap.com," a Citadel Command and Control Domain, to check for most recent configuration file



9. With reference to Figure 1, assume, for example, that the Citadel-infected personal computer is programmed to contact "AnGap.com," a domain that Citadel-infected personal computers have been seen to contact. In Step 1, the infected personal computer contacts a local DNS server, and it asks the local DNS server for the IP address for AnGap.com.

10. In Step 2, the local DNS server contacts an upstream DNS server at a higher level of the DNS hierarchy for that information.

11. In Step 3, the upstream name-server replies to the local DNS server with the IP address of the authoritative name server for AnGap.com, which is ns1.ardniapark.net, at IP address 122.11.226.26.

12. In Step 4, the local DNS server then contacts the ns1.ardniapark.net server at the IP address given and asks for the IP address for the domain AnGap.com.

13. In Step 5, the authoritative name server for AnGap.com replies with the exact IP address for that sub-domain, 192.168.72.57 (this is only an example; it is not the actual IP address).

14. In Step 6, the local DNS server sends that information back to the Citadel-infected personal computer.

15. In Step 7, the Citadel-infected personal computer contacts the computer at 192.168.72.57 and asks if there is a new configuration file.

16. Finally, in Step 8, if a configuration file is available that is newer than the configuration file currently being used by the Citadel bot, the bot will download the newer configuration file. The configuration file, placed on AnGap.com by the botnet operator will generally contain a new set of command and control servers for the bot to communicate with, and will contain other information used by the bot to commit crimes.

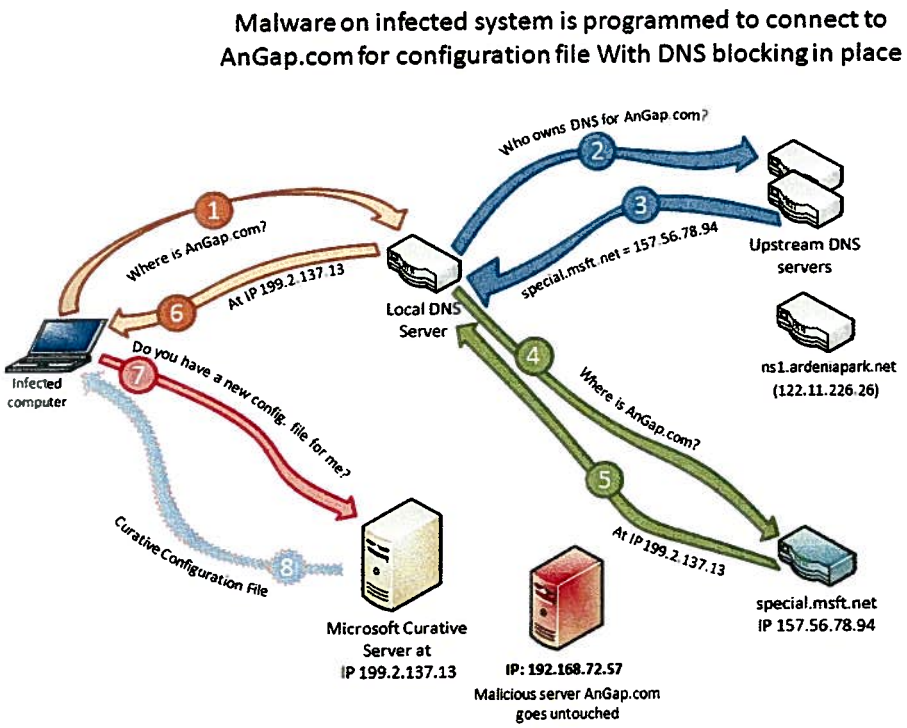
B. Effect Of Court-Ordered Relief

17. If the Court grants the relief Microsoft has requested, two main things will change in the scenario depicted in Figure 1, above. First, anytime an infected end user computer attempts to contact a command and control domain, it will instead be routed to a Microsoft server. Second, the Microsoft server will send the infected end-user computer a configuration file meant to help the end-user remove the Citadel infection. I will describe each part of this in greater detail below.

1. Citadel Infected Computers Will Communicate With Microsoft Curative Servers

18. With regard to currently registered (i.e., active) domains, the requested relief involves changing the authoritative name servers to servers controlled by Microsoft. Once this occurs, when an infected end-user computer attempts to contact its command and control server, it will instead be redirected to a Microsoft Curative Server. This is depicted in Figure 2, below.

Fig. 2



19. In Figure 2, the first two steps are the same as in Figure 1: the infected end-user computer attempts to contact a command and control server called AnGap.com, and the local DNS server queries the upstream DNS server for the IP address of the authoritative name server for AnGap.com.

20. 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.

21. In Step 4, the local DNS server now queries special.msft.net for the IP address of AnGap.com. It never queries the former name server, ns1.ardeniapark.net.

22. In Step 5, special.msft.net responds to the local DNS server with the IP address of the Microsoft Curative Server, in this example 199.2.137.13.

23. In Step 6, the local DNS server sends this IP address back to the infected end-user computer, and in Step 7, the infected end-user computer connects to the Microsoft Curative Server as if it were a command and control server. The real command and control server, AnGap.com and the botnet operator are thus effectively cut off from the bot.

24. In Step 8, the infected end-user computer requests and downloads from the Microsoft Curative Server a new configuration file. I will discuss this in more detail in the following section.

2. The First Curative Configuration File Will Promote Automatic Disinfection Of End-User Computers

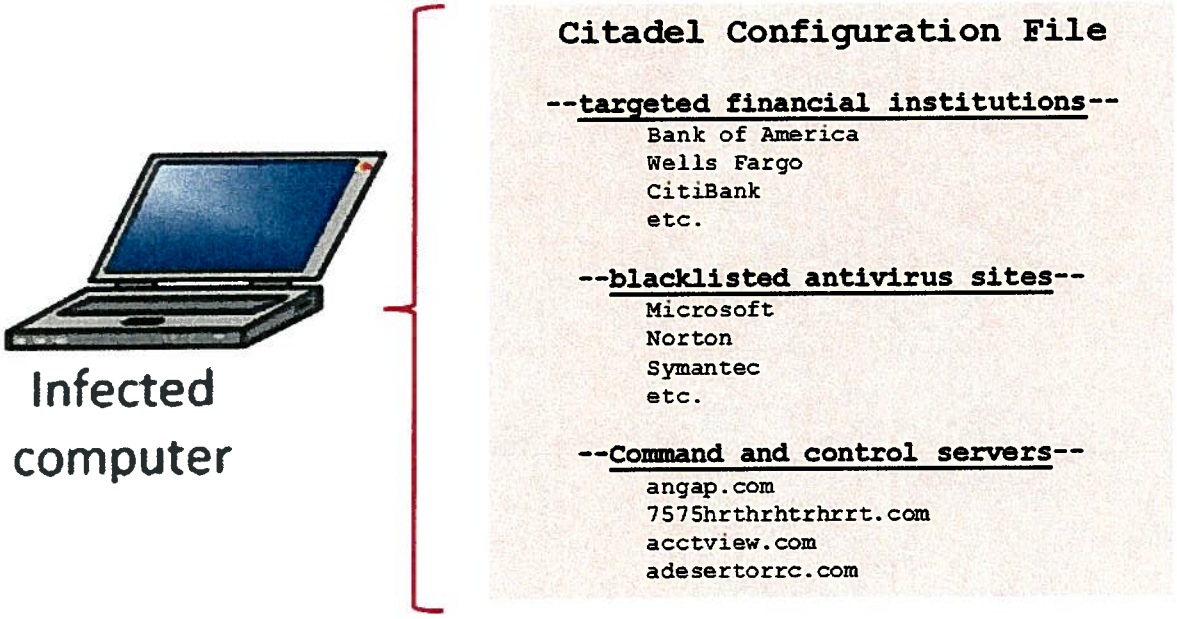
25. Part of the request relief grants Microsoft permission to stage on the Microsoft Curative Server a configuration file meant to "cure" the Citadel infection on the end-user computer. I will refer to this as the "First Curative Configuration File." In other words, once the Order is executed, the scenario depicted in Figure 1 will change to that depicted in Figure 2, and

the infected end-user computers will connect to the Microsoft Curative Server and ask if there is an updated configuration file. The Microsoft Curative Server would, at that point, allow the infected end-user computer to download the First Curative Configuration File. To explain the effect of this, it may be helpful to review the major portions of a typical Citadel configuration file, and then discuss the differences between that and the First Curative Configuration File.

a. A Standard Citadel Configuration File

26. Figure 3, below, shows several major sections of a Citadel configuration file.

Fig. 3.



27. First, the standard Citadel configuration file contains a list of targeted financial institutions. The Citadel malware running on the end-user's computer checks every Internet connection attempted by the end-user against this list, and when it detects a match, it begins logging the user's keystrokes or launches a more sophisticated web inject or other attack.

28. It also contains a blacklist of antivirus websites. This extensive list includes virtually all legitimate vendors or suppliers of antivirus software. Again, the Citadel malware

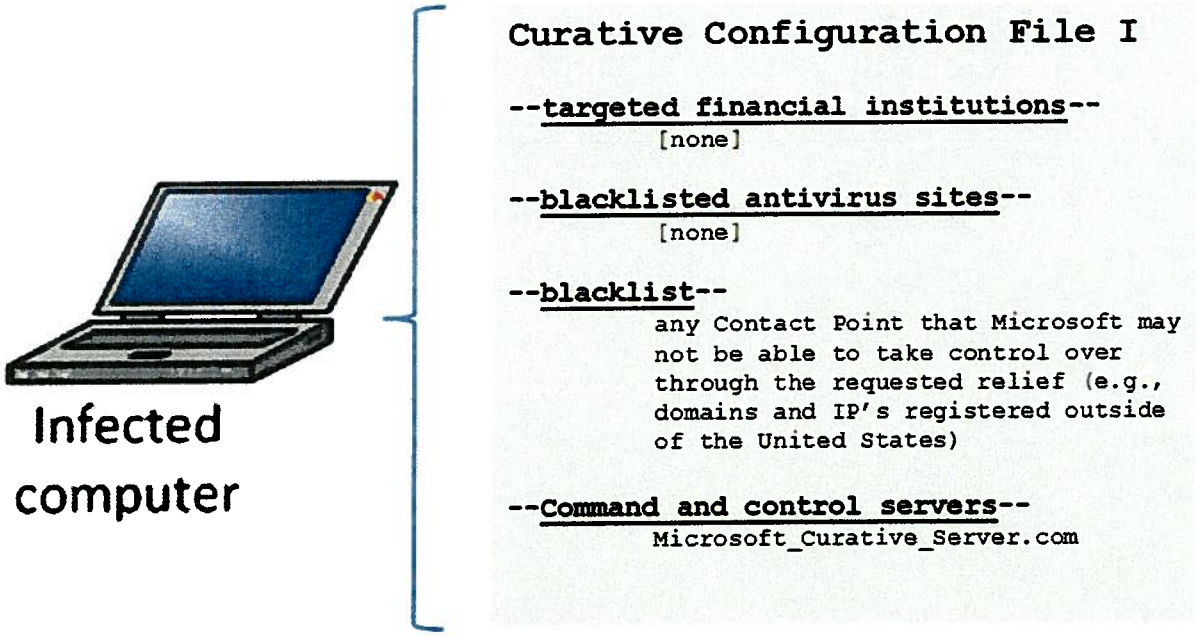
checks any connection attempted by the end-user's computer against this list, and if it detects a match, it hijacks the session and redirects the user's computer to an unrelated website. So, for example, if the user's computer has a standard antivirus software program installed on it, and if that antivirus program attempts to contact the vendor's website to update its signature files, which might contain a signature for Citadel, the Citadel malware will redirect the session and foil the attempted antivirus update.

29. The standard configuration file also contains a list of command and control domains and IP addresses (the "Contact Points") that the malware will attempt to contact every twenty minutes to see if a new configuration file is available.

b. Effect Of The First Curative Configuration File

30. Figure 4, below, represents the contents of the First Curative Configuration File.

Fig. 4



31. The first difference is that the Curative Configuration File will contain no targeted financial institutions. While this does not completely remove the malware running on the

infected end-user's computer, it at least allows the user to communicate with his or her bank without being attacked.

32. The second difference is that there is no blacklist of antivirus websites. Microsoft believes that this will allow most computers with installed antivirus programs with active subscriptions on them to self-clean. The antivirus programs will contact the vendor's website for signature updates, and will download new signature files that will allow the antivirus software to detect and eliminate the Citadel infection. To facilitate this process, Microsoft makes Citadel samples freely available via the Virus Information Alliance, which is a group of leading vendors of antivirus software, so that they can develop the signature files.

33. A third major difference is that there is a black list of any known hard-coded Citadel Contact Points that Microsoft will not control even if given the requested relief. This would include, for example, websites and IP addresses registered outside of the United States. Once the curative configuration file has been downloaded, the Citadel malware on that system will not connect to any of these.

34. Additionally, instead of a list of Citadel command and control servers, the Curative Configuration File will direct the Citadel malware to communicate with the Microsoft Curative Server, which it will do every twenty minutes until it is finally cleansed from the user's computer.

35. Microsoft will keep the First Curative File staged on the Curative Server for at least two weeks following execution of this order. It is believed that during this period of time, the majority of infected end-user computers that are running antivirus software with active subscriptions will be cleansed of the Citadel infection.

3. Effect Of The Second Curative Configuration File

36. After the initial two week period and use of the First Curative Configuration File,

Microsoft anticipates that some subset of end-user computers will continue to be infected with Citadel malware. For example, some end-users undoubtedly will not be running antivirus software on their computers or getting automatic updates to their antivirus signature files. Such computers will likely remain infected with Citadel unless the end-user takes other steps to cleanse the computer. To help these users, part of the requested relief would permit Microsoft, should Microsoft determine it to be necessary and prudent, to stage a "Second Curative Configuration File" on the Microsoft Curative Server for up to a maximum of twenty minutes every five hours, one day per week.

37. Figure 5, below, represents the information that will be in the Second Curative Configuration File.

Fig. 5.

Infected computer

Curative Configuration File II

--targeted financial institutions--
[none]

--blacklisted antivirus sites--
[none]

--blacklist--
any Contact Point that Microsoft may not be able to take control over through the requested relief (e.g., domains and IP's registered outside of the United States)

--Command and control servers--
Microsoft_Curative_Server.com

--Antivirus White list--
Norton
Symantec
Microsoft_Curative_Server.com
etc.

--Instructions to the bot--
IF the user tries to connect to any website not in the White list, connect the user to Notice_of_Infection.com

38. In the second Curative Configuration File, the first four sections are the same as what was already discussed in reference to the First Curative Configuration File. The first difference, however, is a "white-list" of antivirus websites, which also includes the Microsoft Curative Server. The purpose of this whitelist is explained in the next paragraph.

39. The other major difference between the First and Second Curative Configuration Files is that the second one contains information that the Citadel malware will use to limit the connections that the user's computer can make. The malware, of course, continues to monitor every Internet connection the user attempts. Now, however, if the malware detects that the user is attempting to contact any website other than a website in its white-list (i.e., the website of a provider of antivirus software or the Microsoft Curative Server), it will redirect the user to a website that will display a notice, substantially similar to one that Microsoft has used previously in a similar case in which a botnet infection had corrupted the browsers on those computers. This notice will advise the user that they are infected with Citadel and will direct them to resources they can use to cleanse their computer of the infection.

40. Because the malware will operate with this configuration file for twenty minutes, the user will not be able to browse anywhere except to a website in the white-list for that period of time. After the twenty minutes is over, the Citadel malware will check the Microsoft Curative Server to see if a new configuration file is available, and will download the First Curative Configuration File which causes the message to disappear and the user can then browse anywhere, except to locations included in the blacklist portion of the configuration file.

41. Microsoft believes that the steps discussed in this Declaration provide the best means of halting the harm caused by and then eradicating the Citadel botnets.

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 28th day of May, 2013

David Anselmi