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. ________________

BRIEF IN SUPPORT OF MICROSOFT'S *EX PARTE* APPLICATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER, SEIZURE ORDER AND ORDER TO SHOW CAUSE FOR PRELIMINARY INJUNCTION

Plaintiff Microsoft Corporation ("Microsoft" or "Plaintiff") seeks an emergency *ex parte* temporary restraining order ("TRO"), seizure order, and preliminary injunction to halt the growth of the "Citadel" botnets that are causing extreme and continued irreparable harm to Microsoft, its customers, many financial institutions, and the general public. Citadel botnets are computer networks made up of an estimated two to five million end-user computers that have been infected with malicious software. The malicious software puts the infected computers under the control of criminals who send instructions to and receive information from the infected computers over the Internet. These criminals use the Citadel botnets primarily to steal financial credentials and money from the owners of the infected computers, but also use them to send spam email, or anonymously conduct other harmful and unlawful activities.

The damage caused by this criminal conduct is staggering. It is estimated that between two and five million end-user computers have been infected with Citadel. It is further estimated that Citadel botnet operators have stolen millions of dollars by raiding the financial accounts held by the owners of the infected end-user computers at some of the world's leading banks, including Bank of America, Wells Fargo, Citibank, and Chase. The Citadel botnets cause further substantial harm by misusing Microsoft's trademarks to lull the owners of infected end-user computers into believing that their Windows operating system, Internet Explorer and other software are functioning normally, when in fact they have been converted into weapons of crime aimed directly at the end-users' bank accounts.

Citadel is a particularly sophisticated and destructive botnet enterprise. At the core of the enterprise is the Defendant identified as John Doe 1. John Doe 1 develops and sells a software tool, known as the "Citadel Builder Kit," to other cybercriminals over the Internet. The Citadel Builder Kit allows the purchaser to generate the code necessary to create and operate a Citadel botnet. Defendants named herein as John Does 2-82 have purchased the Citadel Builder Kit and have used it to create, deploy and operate over 1300 Citadel botnets around the world, including in the Western District of North Carolina.

The requested TRO directs the disablement and seizure of the Citadel Botnets' command and control servers. These are specialized computers and software located at specific Internet domains and Internet Protocol (IP) addresses, which send instructions to infected end-user computers and steal online credentials and funds from the victims. The command and control software operating from and through these domains and IP addresses instruct infected end-user computers how to perform their day-to-day illegal activities. Disabling the command and control servers will cut communication between the botnet operators and the infected end-user computers thereby bringing to a halt the criminal acts of these Defendants. The requested TRO directs further steps to then neutralize the Citadel code running on the end-users' computers, including removing the lists of targeted financial institutions that Citadel relies upon to steal money, allowing end-users' computers to connect to websites from which they can download anti-virus software (something that Citadel currently blocks them from doing) and communicating instructions to users in their web browsers regarding how to remove the malicious software.

Ex parte relief is essential here. Notice to Defendants would provide them an opportunity to destroy, move, conceal, or otherwise make inaccessible the instrumentalities used to direct the Citadel botnets and the primary evidence of their unlawful activity. Defendants can easily redirect infected end-user computers away from the identified command and control servers if they learn of the impending action. Giving them that opportunity would render further prosecution of this lawsuit entirely fruitless. Equally important, the command and control servers must be disabled simultaneously to prevent one or more Defendants from directing already-infected end-user computers to communicate with alternate command and control servers, allowing the Citadel botnets to continue to operate and harm Microsoft and the public.

The requested *ex parte* relief is not uncommon when disabling dangerous botnets. In a February 2010 case concerning the "Waledac" botnet, the District Court for the Eastern District of Virginia (Judge Brinkema) adopted an approach where:

1) the Court issued a tailored *ex parte* TRO, including provisions sufficient to effectively disable the harmful botnet infrastructure, preserve all evidence of its operations and stop the irreparable harm being inflicted on Microsoft and the public, including Microsoft's customers;

2) immediately after implementing the TRO, Microsoft undertook a comprehensive effort to provide notice of the preliminary injunction hearing and to effect service of process on the defendants, including Court-authorized alternative service by e-mail, electronic messaging services, website publication, mail, facsimile, and treaty-based means; and

3) after notice, the Court held a preliminary injunction hearing, and granted the preliminary injunction while the case proceeded, in order to ensure that harm caused by the botnet could not continue during the action.

See Microsoft v. John Does 1-27, Case 1:10-cv-00156 (E.D. Va. 2010, Brinkema, J.) (orders attached to Declaration of Jeffrey Cox In Support of Microsoft's Motion for a TRO ("Cox Decl."), Exs. 12, 13). Subsequently, in five further cases to disable botnets, the Eastern District of Virginia, the Western District of Washington and the Eastern District of New York granted TROs adopting this approach. *See Microsoft v. John Does, 1-11,* Case No. 2:11-cv-00222 (W.D. Wash. 2011) (Robart, J.) (March 2011 – disabling "Rustock" botnet); *Microsoft v. Piatti, et al.,* Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.) (September 2011 – disabling "Kelihos" botnet); *Microsoft Corp. et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.) (March 2012 – disabling "Zeus" botnets); *Microsoft Corp. v. Peng Yong et al.*, Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.) (September 2012 – disabling "Nitol" botnet); *Microsoft Corp. v. John Does 1-18*, Case No: 1:13-cv-139 (E.D. Va. 2013, Brinkema, J.) (January 2013 – disabling "Bamital" botnet); *see* Cox Decl., Exs. 14-21.

A similar approach is appropriate here. If the Court grants Microsoft's requested relief, upon execution, Microsoft will immediately make a robust effort in accordance with the requirements of Due Process to provide notice of the preliminary injunction hearing and to effect service of process on Defendants. Microsoft will immediately serve the Complaint and all papers in this action on Defendants, using known contact information and contact information maintained by the third-party domain registrars and hosting companies that host Defendants' command and control infrastructure.

I. THE CITADEL BOTNETS PROVIDE A SOPHISTICATED PLATFORM FOR CYBERCRIME

A. Citadel—A Criminal Botnet Enterprise

Microsoft seeks to stop the illegal acts of Defendants, who, among other illegal conduct, break into and take control of the Microsoft operating system and other software on computers of end-users around the world, steal their financial credentials, and then use this information to pilfer their bank accounts. Declaration of Vishant Patel in Support of Microsoft's Motion for TRO ("Patel Decl.") ¶¶4-6; Declaration of Pamela Moore ("Moore Decl.") ¶14; Declaration of Eric Guerrino ("Guerrino Decl.") ¶16. Defendants do so through what is commonly referred to as the "Citadel botnets," or more simply, "Citadel." Patel Decl. ¶4. Theft attributed to Citadel operators has been estimated to be millions of dollars. *Id.* ¶18; Guerrino Decl. ¶10.

A "botnet" is a network of end-user computers that have been infected with a particular type of malicious software ("malware"). Patel Decl. ¶5. This malware places the infected computers under the control of the individuals who operate the botnet. *Id.* The botnet operators communicate with the infected computers over the Internet and use them to conduct their illegal acts. *Id.* Citadel, though recently-emerged in the world of cybercrime, is a highly sophisticated botnet designed to intrude upon Microsoft's Windows operating system and steal money from the financial accounts of individuals whose computers have become infected with the Citadel malware. *Id.*

Citadel inflicts extreme damage on individuals whose computers have been infected by Citadel. *Id.* ¶10. Once infected with Citadel, the online banking activities of these unknowing victims come under the constant surveillance of Citadel's operators, whose goal it is to steal their financial account login IDs, passwords, and other credentials, so as to steal their money and their identities. *Id.*; Guerrino Decl. ¶¶9-11.

Additionally, Citadel inflicts extreme damage on Microsoft and financial institutions whose customers have been victimized by Citadel, and whose trademarks are frequently abused by the botnet operators as part of their fraudulent schemes. Patel Decl. ¶10; Guerrino ¶¶13-14. Citadel inflicts extreme damage on Microsoft by creating and deploying malware specifically designed to attack computers running Microsoft software. Patel Decl. ¶11. Microsoft's brand, trademarks, reputation, and customer goodwill are all damaged by Citadel. *Id.* In addition, Microsoft must deploy significant resources to help its customers defend themselves against Citadel. *Id.*

The software code behind Citadel is the creation of a Defendant whose true identity is unknown and who is therefore identified herein as John Doe 1. *Id.* ¶7. From evidence of John Doe 1's online activities, John Doe 1 most likely operates from and resides in Ukraine or Russia. *Id.*; *see also,* Declaration of Zoe Krumm ("Krumm Decl.") ¶8 (use of unauthorized Windows XP product key used in creating bot code centers primarily in Ukraine and Russia). John Doe 1's business is to develop and sell "Citadel Builder Kits" to other cybercriminals, whose true identities are also unknown and who are therefore identified herein as John Does 2-82. Patel Decl. ¶7. John Does 2-82 have used the Citadel Builder Kits, in combination with a stolen version of Windows XP and an unauthorized product key for Windows XP, both also provided by John Doe 1, to create, deploy, and operate multiple Citadel botnets used to commit financial crimes over the Internet. *Id.* John Doe 1 first offered Citadel at least as early as January 2012 and John Does John Does 2-82 joined the enterprise thereafter.

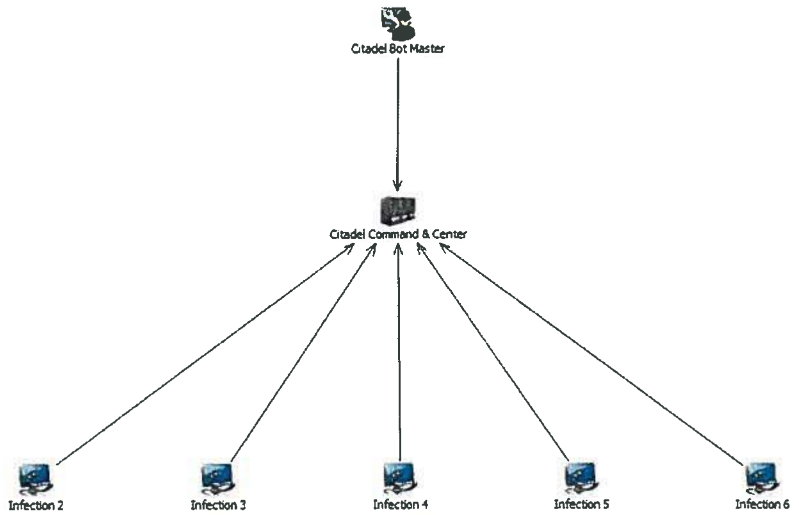
John Doe 1 has won a dark distinction among cybercriminals by providing an unusual degree of after-sales service to his customers. *Id.* ¶8. Using a customer relationship management tool called "Citadel CRM," which is provided over the Internet by John Doe 1, John Does 2-82 communicate with John Doe 1 and with each other regarding updates to Citadel code, support with technical problems, and best practices in deploying, running, and defending their Citadel botnets. *Id.* Using Citadel CRM, John Doe 1 solicits or proposes new feature ideas for Citadel, and John Does 2-82 can vote on which feature or features they would like to John Doe 1 implement, and can offer whatever price they would pay John Doe 1 to induce him to do the work. *Id.* Evidence of online communications between John Does 1-82 demonstrate that they actively collaborate, day-to-day, on the development and operation of Citadel. Moore Decl., ¶14, Ex. E.

In short, the evidence shows that Citadel operates as an enterprise. John Doe 1 develops, commercializes, and supports the Citadel builder kits. He continuously cooperates with and supports John Does 2-82, who have purchased the builder kits and who have created and deployed one or more Citadel botnets with them. John Does 2-82 in turn continuously give feedback to John Doe 1 as to how to continue to develop the Citadel codebase, and pay John Doe 1 to make continuous improvements to the Citadel code base. Patel Decl. ¶9.

B. <u>The Organization, Structure And Function Of A Citadel Botnet</u>

Citadel botnets have a two-tiered architecture. *Id.* ¶17. The lowest tier is referred to as the "Infection Tier," which is made up of bots running on infected end-user computers. *Id.* The second tier is a "Command and Control Tier" through which the botnet operator communicates with and controls the bots. *Id.* The tiered architecture of the Citadel can be represented as shown in Figure 1, below (*id.*):

Fig. 1



1. **The Citadel Infection Tier**

The Infection Tier consists of an estimated two to five million infected end-user computers, which are, unbeknownst to their owners, under the control of a Citadel botnet operator. *Id.* ¶18. These end-user computers are of the type commonly found in businesses, living rooms, schools, libraries, and Internet cafes around the world. *Id.* These computers are commonly referred to as Citadel "bots." Defendants target the owners of such computers and steal financial account credentials and other personal information from them. Defendants have intentionally placed Citadel bots on infected end-user computers throughout the United States, including in the Western District of North Carolina. Patel Decl. ¶¶19-20.

2. **The Citadel Command and Control Tier**

The second level of the Citadel botnet architecture is referred to as the "Command and Control Tier." *Id.* ¶21. This consists of specialized computers, also connected to the Internet, which run specialized software. *Id.* Defendants have purchased or leased these servers and use them to send commands to control the infected computers in the Infection Tier and to receive information from the infected computers. *Id.*

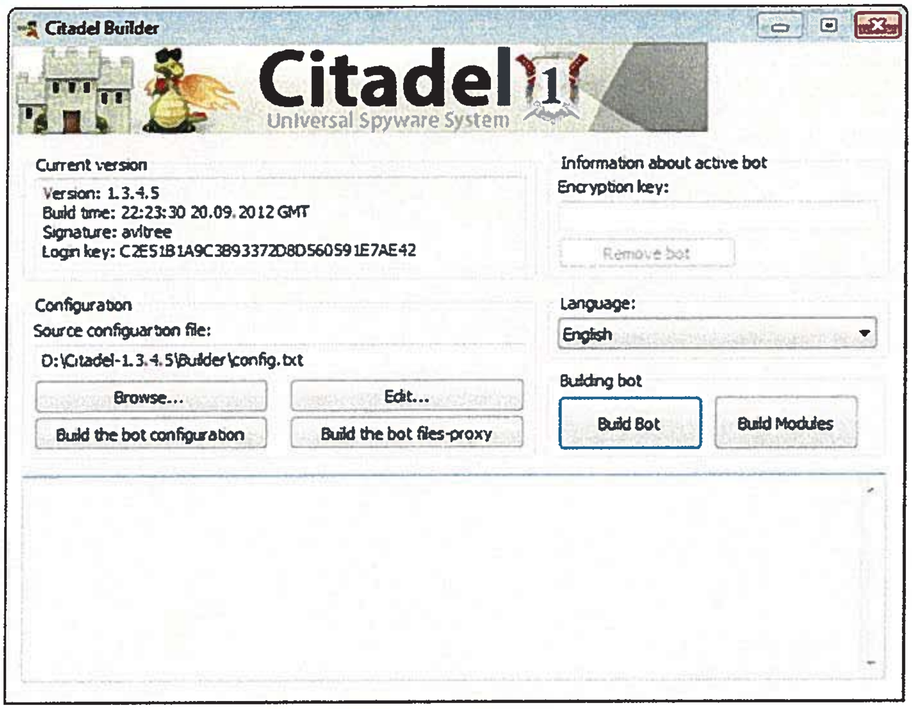
The Citadel-infected end-user computers—the bots—are caused by the Citadel malware running on them to periodically connect over the Internet to one or more command and control servers, typically every 20 minutes. *Id.* ¶¶22, 47; Declaration of David Anselmi ("Anselmi Decl.) ¶4. The bots download updates and instructions from, and upload information to, these servers. By updating the instructions placed on the command and control servers, Citadel botnet operators are able to communicate with and control the Citadel-infected end-user computers. Patel Decl. ¶22. Servers in the command and control tier include the servers at the domain names and IP addresses at Exhibits 2 and 3 to the Patel Declaration. *Id.* ¶23.

C. Creation, Propagation, And Operation Of Citadel Botnets

1. Creation Of Citadel Botnet Code And Configuration File

To create a Citadel botnet, a criminal begins by purchasing a Citadel Builder Kit from John Doe 1. *Id.* ¶26. The Builder Kit is a software application that guides the purchaser through a series of options which will determine how the Citadel botnet code will be configured. *Id.* After determining the configuration settings, the purchaser can push a "Build Bot" button, and the builder kit will create both the executable botnet code as well as configuration files that the botnet operator will place on command and control servers. Patel Decl. ¶26. In Citadel's lexicon, the "bot" is the module that will be downloaded onto an end-user's computer to infect and control it. *Id.* The configuration file is a text file that contains parameters that the bot will use to control its day-to-day work, such as what domains to connect to. *Id.* Figure 2, below, shows a screen shot taken from a Citadel Builder Kit.

Fig. 2



Version: 1.3.4.5
Build time: 22:23:30 20.09.2012 GMT
Signature: avltree
Login key: C2E51B1A9C3B93372D8D56059 1E7AE42

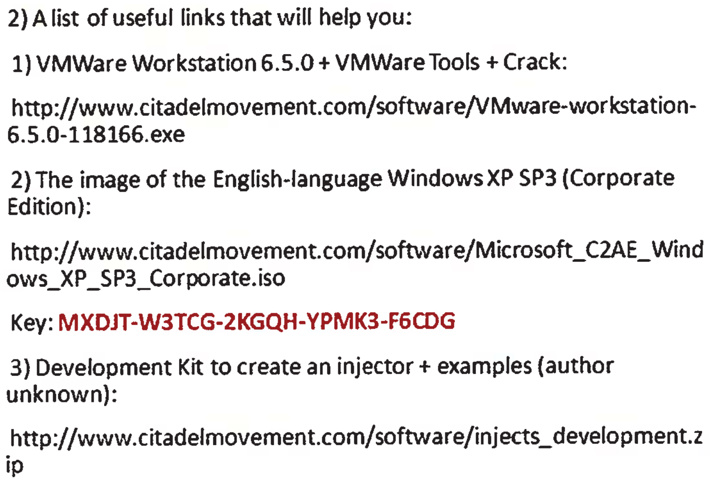
Encryption key:

Source configuartion file:
D:\Citadel-1.3.4.5\Builder\config.txt

Language: English

John Doe 1 urges his customers to build the bot code on computers running Windows XP. *Id.* ¶27. This ensures that all Citadel bots are built in a common environment, making it easier for John Doe 1 to test the Citadel build kits. *Id.* In order to provide his botnet customers with access to Windows XP without having to pay Microsoft for it and presumably better obfuscate his identity, John Doe 1 provides a stolen version of Windows XP and a unauthorized product key for Windows XP. *Id.* ¶28. Figure 3, below, shows a section taken from the Citadel build kit manual. *Id.* It gives Citadel customers a path (no longer active) to a stolen version of Windows XP, and it provides, in red, an unauthorized product key for that copy of Window XP. *Id.*; Krumm Decl. ¶¶6-7.

Fig. 3



2) A list of useful links that will help you:

1) VMWare Workstation 6.5.0 + VMWare Tools + Crack:

http://www.citadelmovement.com/software/VMware-workstation-6.5.0-118166.exe

2) The image of the English-language Windows XP SP3 (Corporate Edition):

http://www.citadelmovement.com/software/Microsoft_C2AE_Windows_XP_SP3_Corporate.iso

Key: MXDJT-W3TCG-2KGQH-YPMK3-F6CDG

3) Development Kit to create an injector + examples (author unknown):

http://www.citadelmovement.com/software/injects_development.zip

2. <u>Creation Of Citadel Command And Control Infrastructure</u>

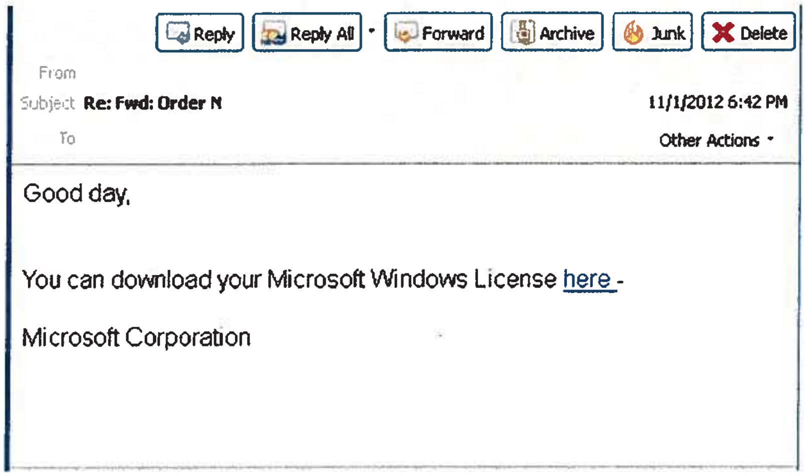
In addition to the code and configuration files created using the Citadel Builder Kit, a Citadel botnet operator needs to set up a command and control infrastructure on the Internet. Patel Decl. ¶29. This is done by setting up accounts with web-hosting providers, which are companies, usually legitimate, that provide facilities where computers can be connected through high-capacity connections to the Internet. *Id.* A Citadel botnet operator may use hundreds of computers connected through various webhosts around the world to provide a command and control infrastructure for his or her botnets. *Id.* The most vulnerable points in the Citadel botnet architecture are the domain names and IP addresses of the command and control servers, as they can be identified and located, and if they are disconnected from the Internet, the botnets' communications with infected end-user computers will be severed (i.e., communications between computers in the Infection Tier and Command and Control Tier will be broken) and the activity of the botnet disabled. *Id.* ¶31.

3. <u>Propagation And Control Of Citadel Botnets</u>

Once a Defendant has created the Citadel bot code, the configuration files, and the command and control infrastructure, he or she infects end-user computers to become Citadel bots. The Defendants use several methods to do this. Patel Decl. ¶32. Typically, the infection of end-user computers involves using software called a "Trojan downloader" that installs the Citadel botnet code on the user's computer. *Id.* The botnet operator will typically stage the Trojan downloader on a website that the botnet operator has set up, or that the botnet operator has broken into. *Id*; Moore Decl. ¶¶19-20. Under normal circumstances, the set of domains and IP addresses associated with the Trojan downloader changes every 7-10 days. Patel Decl. ¶46.

The Defendants then typically use lures to cause individuals browsing the Internet to visit these servers. *Id.* ¶33. In one method, the Defendants send Internet users "spam" emails containing links to the domain names or IP addresses of the servers containing the malicious software. *Id*; Moore Decl. ¶¶4, 7, 18-21; Guerrino Decl. ¶17; Declaration of John Wilson ("Wilson Decl.") ¶¶8-9. The content of the spam email misleads Internet users to click on the links, causing the malicious software to be installed on their computers without their knowledge or consent. Patel Decl. ¶33; Moore Decl. ¶¶7, 18-21; Wilson Decl. ¶¶8-9. Figure 4, below, is an example of this spam. Patel Decl. ¶33. It can be seen from this that the Citadel botnet operators misuse the trademarks of well known companies and organizations such as Microsoft, NACHA and financial institutions and others to fool the recipient into thinking the spam e-mail is from a legitimate source. *Id.* ¶34; Guerrino Decl. ¶17; Wilson Decl. ¶¶8-9. *See, generally*, Moore Decl. ¶¶. 7-21 (describing the use of spam that abuses the NACHA trademark in order to deceive banking customers).

Fig. 4



Re: Fwd: Order N

11/1/2012 6:42 PM

Good day,

You can download your Microsoft Windows License here -

Microsoft Corporation

Once an end-user connects to the website where the Citadel downloader is staged, a highly specialized piece of software staged on that website known as an "exploit pack" will probe the user's computer for vulnerabilities such as might be found in an out-of-date, unpatched operating system, or more likely than not an unpatched application. Patel Decl. ¶35; Moore Decl. ¶18(b)-(c) If a vulnerability is found, the exploit pack will download the Trojan onto the end-user's computer. Patel Decl. ¶35. This will result in the installation of the Citadel bot on the end-user's computer. *Id.* From that point forward, the end-user's computer and the Microsoft Windows operating system running on the computer are secretly controlled by the operator of the Citadel botnet. *Id.* They are, in fact, converted into weapons of crime aimed directly at the end-user's bank accounts. *Id.*

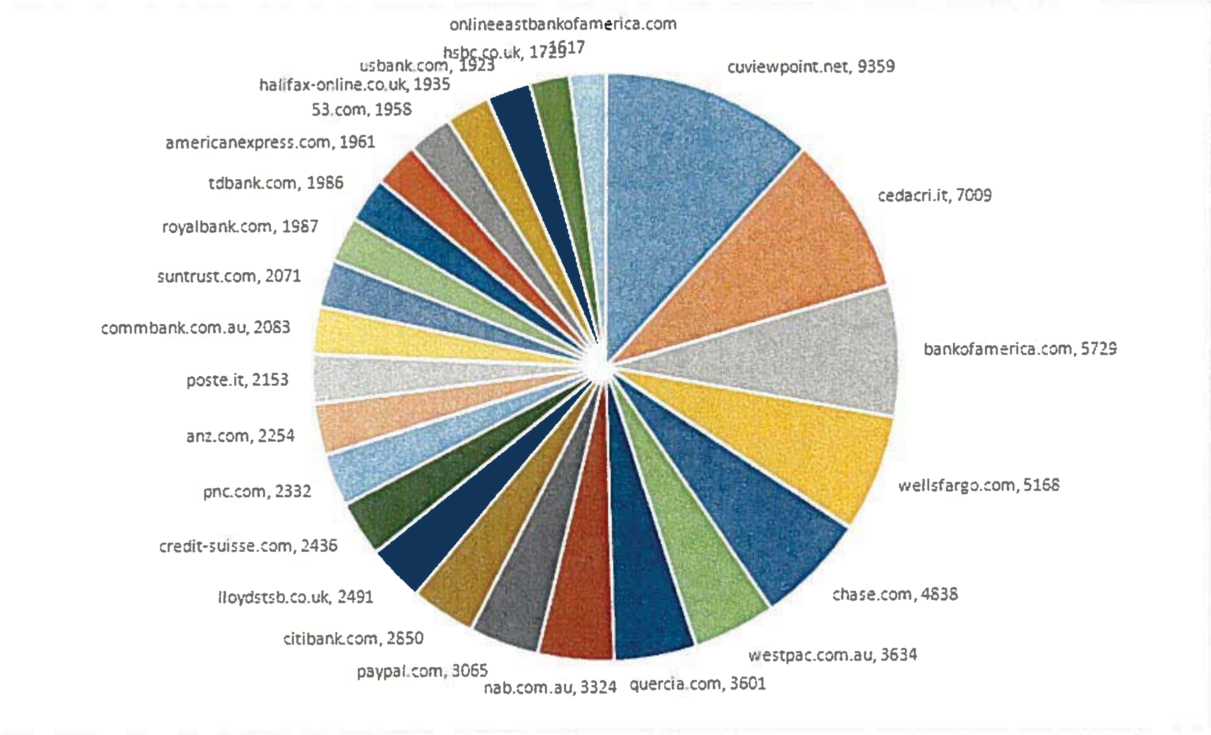
After it is installed, a Citadel bot is programmed to contact one to five command and control computers on the Internet. *Id.* ¶36. These are referred to as the "base domains," because they are the first domains that a Citadel bot will attempt to contact, and they are included in the original bot executable generated by the Citadel Builder Kit. Patel Decl. ¶36. By studying many thousands of Citadel bots, Microsoft has developed a list of these base domains. *Id.*, Ex. 5

When a Citadel bot establishes contact with one of these base domains, the bot will download an encrypted configuration file from it. *Id.* ¶37. Citadel configuration files contain various types of information which will control the operation of the bot on the end-user's computer. *Id.*; Anselmi Decl. ¶¶4-5, 26-29. By changing the configuration files, the operators of Citadel can control the operation of the infected end-user computers. Patel Decl. ¶37; Anselmi Decl. ¶¶4-5. The domains listed in Exhibit 6 to the Patel Declaration host the Citadel configuration files. Patel Decl. ¶37.

Citadel configuration files contain a variety of information used by the bot in the day-to-day work of stealing money. *Id.* ¶¶37-38; Anselmi Decl. ¶¶4-5, 26-29. Most significant is a list of targeted financial institutions. The Citadel bot running on an infected end-user computer will monitor all Internet connections attempted by the end-user, waiting for the end-user to attempt to connect to one of the listed financial institutions. Patel Decl. ¶¶38-39; Anselmi Decl. ¶¶26-27. At that point, the bot can begin its attack on the user's accounts using a variety of techniques discussed below. Patel Decl. ¶38; Anselmi Decl. ¶27.

By studying many configuration files, Microsoft has developed a list of the financial institutions attacked by the various Citadel botnets in operation. *Id.* ¶¶38-39, Exs. 8-9. Figure 5, below, shows the number of times each of the top 25 Citadel targets has been listed in a captured configuration file. *Id.* ¶39. Bank of America, Wells Fargo, Chase, Citibank, American Express, and U.S. Bank are among the top United States-based financial institutions targeted by Citadel. Bank of America, of course, is headquartered in Charlotte, North Carolina. *Id.*

Fig. 5



Second, a Citadel configuration file will contain a list of Citadel Command and Control servers with which it is to communicate. *Id.* ¶41; Anselmi Decl. 29. It will contact these Command and Control computers to download updated configuration files, updated software, and new attack modules; and it will also use these Command and Control computers to upload information stolen from the end-user. *Id.* ¶41. Exhibits 2 and 3 to the Patel Declaration contain a true and correct list of Citadel Command and Control servers of this type. *Id.* The command and control servers that the installed bots communicate with are changed-over every six to eight weeks and replaced with new command and control servers, making the botnet's infrastructure a moving target. *Id.* ¶46.

Additionally, a Citadel configuration file will contain information that the bot will use to keep from attacking end-users or financial institutions in Ukraine or Russia. *Id.* ¶44. It is commonly believed that the creators of Citadel include this information so as to keep Citadel botnets from being active in the countries in which they operate so as to avoid provoking local law enforcement action against themselves. *Id.*

4. Defensive Mechanisms Of Citadel Botnets

Relevant to the relief Microsoft seeks, Citadel botnets have certain defensive mechanisms to better withstand technical counter-measures. Patel Decl. ¶¶45-51. The first is the ability of Citadel's operators to change to a completely new command and control infrastructure very quickly if they detect an attack on the botnet infrastructure. *Id.* ¶47. Because the bots check with the command and control servers for a new configuration file every 20 minutes, and because the botnet operators can deploy new configuration files around the world almost instantaneously, the botnet operators are able to quickly move the bots over to a new command and control infrastructure if they detect an attack has started on the existing command and control infrastructure. *Id.*

An additional mechanism is that the Citadel bot running on the end-user computer will keep that computer from connecting to websites associated with anti-virus software. *Id.* ¶50; Anselmi Decl. ¶¶26, 28. If a user attempts to connect to a website from which to download anti-virus software, Citadel will block that. Patel Decl. ¶50; Anselmi Decl. ¶28. When the Citadel bot detects an attempt to connect to an antivirus website, it will hijack and redirect the user's browser. Patel Decl. ¶50; Anselmi Decl. ¶28. This keeps any antivirus software on the user's computer from receiving updates, and it prevents victims from being able to visit antivirus or other security sites to download removal tools and obtain mitigation advice. Patel Decl. ¶¶49-50, Exs. 10, 11; Anselmi Decl. ¶28.

D. Defendants Use Citadel To Steal Money

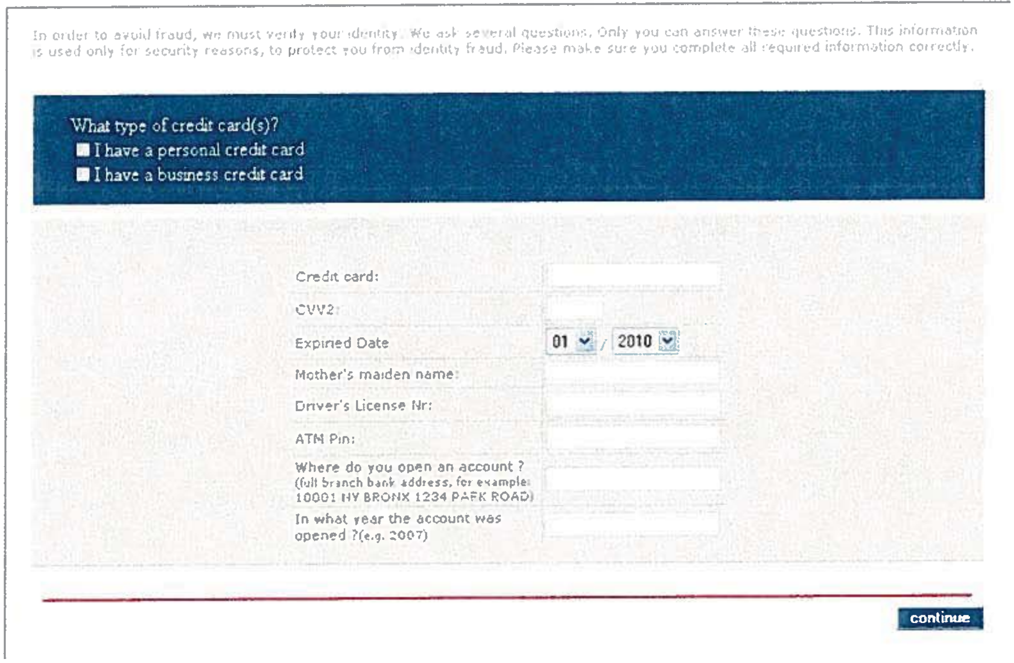
As soon as a Citadel botnet is operational, Defendants move to the next phase: stealing money from the financial accounts of the owners of the infected end-user computers. A Citadel attack begins when the Citadel bot running on the infected end-user computer detects that the user is attempting to connect to the website of a financial institution. Patel Decl. ¶53. Once the Citadel bot detects that the user has attempted to connect to a targeted financial website, the bot can proceed in several ways. *Id.* ¶54. First, it can log the keystrokes entered by the user while the user accesses their financial accounts, it can record information displayed by the website, and it can even take screenshots or a video of what the user's account pages look like. *Id.*; Moore Decl. ¶7. The Citadel bot will upload all of this information later to a command and control server, at which point the botnet operator can retrieve it and use it to steal from the user's accounts or conduct other illegal acts with the stolen information. Patel Decl. ¶54.

In a variation on this basic attack, the Citadel bot running on the infected end-user computer can use a technique called a "web-inject" to extract more sensitive information from the user. *Id.* ¶55. In a web-inject attack, the Citadel bot alters the appearance of the webpage of the financial institution as it is displayed in the end-user's browser. In essence, the Citadel bot takes control of the user's browser, and instead of allowing the browser to provide an accurate rendering of the website to which the user has connected, it causes the browser to change what the user sees. *Id.* It does this by "injecting" additional code into the website code that the browser is rendering in a displayable format for the user. *Id.*

For example, if the real website asks only for a login ID and password, the bot can extend it through a web-inject attack 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. *Id.* ¶56. Citadel is capable of exploiting various browsers in this manner including

Microsoft Internet Explorer, Google Chrome, and Mozilla Firefox. *Id.* Figure 6, below, shows a screen-shot of what an example Citadel "web inject" looks like. *Id.* ¶63. In this case, the Citadel bot operator was attempting to gather credit card account information from the victim and other personal information that could also be used in identity theft. *Id.*

Fig. 6



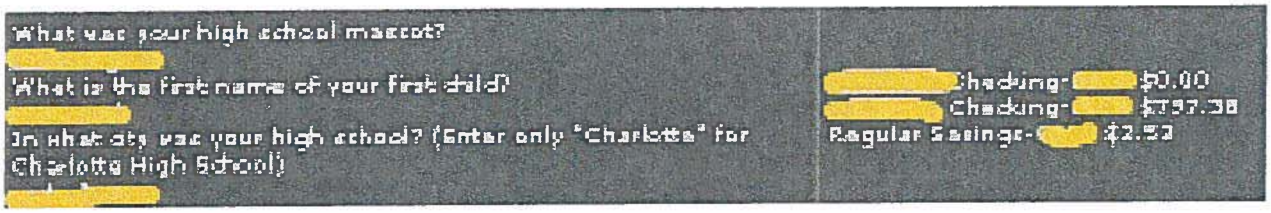
In order to avoid fraud, we must verify your identity. We ask several questions. Only you can answer these questions. This information is used only for security reasons, to protect you from identity fraud. Please make sure you complete all required information correctly.

What type of credit card(s)?
☐ I have a personal credit card
☐ I have a business credit card

Credit card:
CVV2:
Expired Date 01 / 2010
Mother's maiden name:
Driver's License Nr:
ATM Pin:
Where do you open an account ? (full branch bank address, for example: 10001 NY BRONX 1234 PARK ROAD)
In what year the account was opened ?(e.g. 2007)

Figure 8, below, shows a Citadel console used by a botnet operator to organize and display stolen credit card information and personal information, which has been redacted. Patel Decl. ¶64.

Fig. 8



What was your high school mascot?
[redacted]
What is the first name of your first child?
[redacted]
In what city was your high school? (Enter only "Charlotte" for Charlotte High School)
[redacted]

[redacted] Checking-[redacted] $0.00
[redacted] Checking-[redacted] $737.38
Regular Savings-[redacted] $2.53

In another version of this attack, the Citadel bot can display a completely fake website for the financial institution the end-user is attempting to contact. *Id.* ¶57; Guerrino Decl. ¶17. To do this, it first hijacks the user's browser to keep it from connecting to the real website of the financial institution. Patel Decl. ¶57. It then contacts a command and control server and downloads a template for the website of the financial institution and displays that to the user or connects the user to a fake website. *Id.* ¶¶57-58. The user, believing he is connected to the real website of the financial institution, proceeds as normal. However, while the user types in their real account access information such as login ID and password into the fake website, the botnet operator can access their accounts on the real website. *Id.* ¶57. Altered account information from the real website can be reflected back to the user looking at the false website so as to maintain the ruse until the theft is complete. *Id.* To complete the theft, the botnet operator can alter the transactions performed on the real website by, for example, changing withdrawal amounts and changing information related to where the money is to be sent. Patel Decl. ¶57. The botnet operators repeatedly misuse the trademarks of financial institutions on these fake online banking websites in order to confuse and mislead victims. *Id.* ¶59. This makes it nearly impossible for users to detect the attack. *Id.*

Worse, Citadel bots allow the botnet operator to remotely access and operate the infected computer over the Internet. *Id.* ¶60. The botnet operator can connect the end-user's computer to the end-user's bank and use the login information previously stolen from the end-user to empty the end-user's bank accounts. Patel Decl. ¶¶60-61. The malicious software is specifically designed to allow Defendants to conduct this malicious activity without revealing any evidence of the fraud to the end-user, Microsoft, the financial institutions or other victim websites until it is too late for the user or owners of these websites to regain control over funds or stolen information. *Id.* ¶62. For example, to avoid alerting the end user to the activity being conducted remotely via their own computer, the Citadel bot has a command to turn off any sounds (e.g., beeps or clicks) that the end-user's computer might otherwise make while being operated remotely. *Id.*

Beyond stealing from the financial accounts of an infected end-user, once a computer is infected with Citadel, it is more susceptible to being infected with still other types of malware also designed to steal money from the end-user. *Id.* ¶¶65-67.

E. Defendants Use End-User's Computers To Attack Other Computers On The Internet

Some versions of Citadel provide a module meant to enlist the infected computer in a particular type of attack known as a distributed denial of service ("DDoS") attack. *Id.* ¶68. In a DDoS attack, thousands of infected end-user computers connected to the Internet will be marshaled by the botnet operator to simultaneously and continuously attempt to connect to the targeted website. Patel Decl. ¶68. This will make it impossible for legitimate customers to connect to the website, and such attacks are frequently used to extort money from businesses or to exact revenge. *Id.* Citadel bot operators also time DDoS attacks on financial institutions to divert the attention of the bank away from a theft that is occurring or has occurred. *Id.*

F. Damage To Computers And Microsoft Software

Aside from the harms listed above, the Citadel infection itself harms Microsoft and Microsoft's customers by damaging the customers' computers and the software installed on their computers licensed from Microsoft. *Id.* ¶69. During the infection of an end-user's computer, the malicious software makes changes at the deepest and most sensitive levels of the computer's operating system. *Id.* ¶¶69-76. When the Citadel executable infects a targeted computer, it disables the Windows firewall, removes Microsoft Security Essentials, and adds new users or escalates privileges of the current users. *Id.* ¶71. Additionally, it makes fundamental changes at the level of the Windows Registry. *Id.* ¶¶70-71. 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. *Id.* ¶¶73-76.

In effect, once infected, altered and controlled by Citadel, the Windows operating system and Internet Explorer browser cease to operate normally and are now tools of deception and theft aimed at the owner of the infected computer. *Id.* ¶74. Yet they still bear the Microsoft Windows and Internet Explorer trademarks. *Id.* This is obviously meant to and does mislead Microsoft's customers, and it causes extreme damage to Microsoft's brands and trademarks. *Id.* Customers are usually unaware of the fact that their computers are infected and have become part of the Citadel botnet. *Id.* ¶75. Even if aware of the infection, they often lack the technical resources or skills to resolve the problem, allowing their computers to be misused indefinitely. *Id.* ¶76. Even with professional assistance, cleaning an infected end-user computer can be exceedingly difficult, time-consuming, and frustrating. *Id.* ¶76, Exs. 18, 19.

1. <u>Citadel Causes Severe Injury To Microsoft</u>

Microsoft, as a provider of the Windows® operating system and Internet Explorer® web browser, must incorporate security features in an attempt to stop account credential theft by the Citadel botnets from occurring to customers using Microsoft's software. *Id.* ¶77. Additionally, Microsoft devotes significant computing and human resources to combating infections by the Citadel and helping customers determine whether or not their computers are infected, and if so, cleaning them. *Id.* ¶78. Customers' frustration with having to deal with Citadel Botnet infections on their computers, discussed above, unfairly diminishes their regard for Windows and Microsoft, and tarnishes Microsoft's reputation and goodwill. *Id.* ¶79.

2. **The Citadel Botnets Cause Severe Injury To Third Parties And The Public**

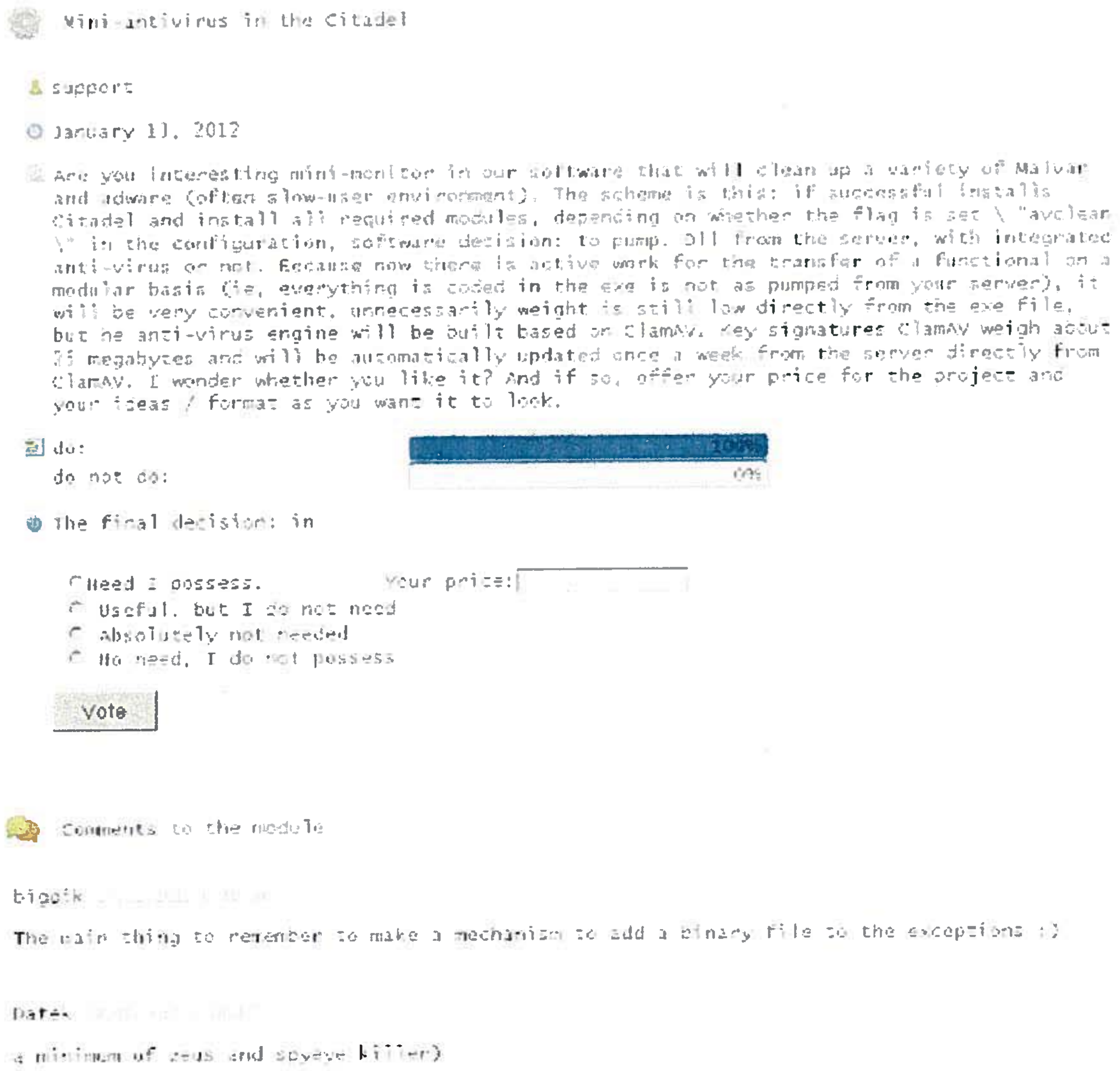
Citadel causes injury to numerous financial institutions, whose interests are represented by the trade groups FS-ISAC and American Bankers Association, as well as NACHA, the administrator of the ACH electronic funds transfer systems, and Microsoft and its individual customers whose information and funds are stolen. *Id.* ¶80; Moore Decl. ¶¶2, 12, 15; Guerrino Decl. ¶17. For example, in 2012, NACHA has seen several spam campaigns of the type utilized by operators of Citadel botnets. Moore Decl. ¶9. These are "socially-engineered" spam campaigns organized around normal monthly business payment processing dates, which is a ruse to induce the recipients of the spam e-mail to believe they are legitimate. *Id.* In 2013, two spam campaigns were launched in mid-February and the first week in April with average spam e-mails of the type used by operators of Citadel of 3.7 million e-mails per event. *Id.* These spam campaigns abuse NACHA's trademark. *Id.*, Ex. A.

In response, NACHA has been required to expend considerable resources to track and attempt to counter the threat posed by these sorts of attacks. *Id.* 9-13. They have damaged the reputation of NACHA and other financial institutions, and make users more hesitant to use the ACH network, which is the backbone for the electronic movement of money and related information between financial institutions in the United States, or any other online financial service. *Id.* ¶¶3, 12; Guerrino Decl. ¶¶19-20; Wilson Decl. ¶10.

G. **The Global Cybercrime Enterprise Promoting And Operating Citadel**

Citadel botnets are run as an enterprise in which all of the Defendants participate in and fund development and improvement of Citadel as a cybercrime operation. John Doe 1 provides an online portal called Citadel CRM ("CRM" is an acronym for "customer relationship management"), where customers can report problems, propose and suggest and vote on new features, and exchange ideas and best practices with other Citadel botnet operators. Patel Decl. ¶¶81-82. Figure 9, below, shows a screen shot of the Citadel CRM. *Id.* ¶82.

Fig. 9



Mini-antivirus in the Citadel

support

January 13, 2012

Are you interesting mini-monitor in our software that will clean up a variety of Malvar and adware (often slow-user environment). The scheme is this: if successful installs Citadel and install all required modules, depending on whether the flag is set \ "avclean \" in the configuration, software decision: to pump. Dll from the server, with integrated anti-virus or not. Because now there is active work for the transfer of a functional on a modular basis (ie, everything is coded in the exe is not as pumped from your server), it will be very convenient, unnecessarily weight is still low directly from the exe file, but he anti-virus engine will be built based on ClamAV. Key signatures ClamAV weigh about 35 megabytes and will be automatically updated once a week from the server directly from ClamAV. I wonder whether you like it? And if so, offer your price for the project and your ideas / format as you want it to look.

do: 100%

do not do: 0%

The final decision: in

○ Need I possess. Your price:

○ Useful, but I do not need

○ Absolutely not needed

○ No need, I do not possess

Comments to the module

bigpik

The main thing to remember to make a mechanism to add a binary file to the exceptions :)

Dates

a minimum of zeus and spyeye killer)

As can be seen from this dialog, John Doe 1 proposed a new feature on January 13, 2012 and solicited the feedback of John Does 2-82. *Id.* ¶83. The proposed feature is giving Citadel bots their own antivirus capability that would allow them to clean other malware infections and "adware" off the end-user's computer. *Id.* ¶84. By removing competing malware, the operators of Citadel botnets hope to make it less likely that the end-user would detect an infection on their computer—something that could cause the end-user to thoroughly clean the computer, and to remove software that could be harming the performance of the Citadel bot on the computer. *Id.* ¶84. The post asks John Does 2-82 to vote on whether the feature would be useful or not, and invites them to offer a price for the project. *Id.* ¶83.

John Doe 1 has been diligent in adding new features and fixing bugs and has released multiple versions on a fast schedule to provide the Citadel botnet operators with the latest updates. *Id.* ¶87. In the first six months that Citadel was available, for example, John Doe released five versions of the build-kit. *Id.* ¶83. The fast pace of updates demonstrates the intensity and the amount of work being done to make Citadel a robust implement of cybercrime and the level of cooperation between the Citadel developers and their customers. *Id.* ¶87; Moore Decl. ¶14

In summary, Microsoft's investigation shows that John Doe 1 is the developer of Citadel. *Id.* ¶¶88-89. He has developed and commercialized Citadel by

- designing and developing the Citadel bot code and all of the modules that enable a Citadel bot to conduct theft;
- creating a Citadel Builder Kit that customers can purchase and then use to quickly generate bots and configuration files, which are the primary means of conducting financial theft;
- selling the Citadel Builder Kit in an online Citadel store to other criminals; and providing after-sales service and support to their customers in the form of bug fixes, new features, frequently updated versions of Citadel; and
- offering to collaborate and work-for-hire to add new features. Patel Decl. ¶89.

Microsoft's investigation has also shown that there are 81 Citadel botnet operators, among them deploying over 1300 Citadel botnets. *Id.* ¶¶90-96. Each of John Does 2-82 has participated in the Citadel enterprise through the following acts:

- Purchasing one or more Citadel Builder Kits and using them to generate bots and configuration files to control the bots;
- Deploying the bots in one or more botnets;
- Creating one or more command and control infrastructures made of server computers connected to the Internet through which to communicate with the deployed bots;
- Using one or more means to cause end-user computers to become infected with Citadel;
- Using the Citadel bots infecting the computers of end-users around the world to steal security identification and financial account information;
- Using Citadel bots to steal money directly from the financial accounts of unsuspecting end-users around the world;
- Damaging Microsoft-owned and licensed software including Windows and Internet Explorer, corrupting the behavior of these programs to convert them to instruments of criminality;
- Exploiting Microsoft's famous brands and trademarks in order to mislead Microsoft's customers, and consequently causing severe harm to Microsoft's brands, trademarks, reputation and goodwill;
- Using Citadel bots to send illegal spam e-mail;
- Using Citadel bots to cause secondary infections, such as by the "Reveton" ransomware, which demands payment to unlock the victim computer; and
- Using Citadel bots to launch distributed denial of service attacks on financial and

other institutions. Patel Decl. ¶¶95-96.

II. LEGAL ARGUMENT

Microsoft seeks an *ex parte* TRO, seizure order and preliminary injunction pursuant to Federal Rule of Civil Procedure 65, Section 1116 of the Lanham Act and the Court's inherent equitable authority to prevent compounding the harm caused by the Citadel Botnets and to maintain the *status quo* by ensuring that evidence of Defendants' misconduct is preserved during the pendency of this case. Microsoft's requested relief is warranted here.

A. An *Ex Parte* TRO And Preliminary Injunction Redirecting The Harmful Domains And IP Addresses To Secure Computers And Disabling The Botnet Software Is Warranted

Microsoft seeks a TRO, seizure order and preliminary injunction pursuant to Rule 65(b) to redirect the Harmful Domains and IP Addresses operating the Citadel Botnets to secure computers, such that they are disabled and the evidence of Defendants' misconduct and damage is preserved and the botnet software is disabled on end user computers. To be eligible for preliminary equitable relief, the movant must establish (1) likelihood of success on the merits, (2) that it will be irreparably harmed absent temporary injunctive relief, (3) the balance of equities tips in its favor, and (4) that an injunction is in the public interest. *Winter v. Natural Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008); *Pashby v. Delia*, 709 F.3d 307, 320 (4th Cir. 2013). Specifically, in the Fourth Circuit, courts must consider each *Winter* factor separately and each factor must be satisfied. *See The Real Truth About Obama, Inc. v. FEC*, 575 F.3d 342, 347 (4th Cir. 2009), *vacated on other grounds*, *Citizens United v. FEC*, 558 U.S. 310 (2010), *aff'd, The Real Truth About Obama, Inc. v. FEC*, 607 F.3d 355 (4th Cir. 2010) (per curiam).

The relief requested by Microsoft is warranted. There is a very high likelihood that Microsoft will succeed on the merits. Defendants' intrusion into the protected computers of

Microsoft, financial institutions and millions of individual victims, theft of millions of dollars from innocent Internet users, sending of hundreds of millions of spam emails, and the repeated and deceptive infringement of Microsoft's and third-parties' trademarks violates the Computer Fraud & Abuse Act, the CAN-SPAM Act, the Electronic Communications Privacy Act, the Lanham Act, and the Racketeer Influenced and Corrupt Organizations Act. Defendants' deceptive, misleading, and tortious conduct, moreover, violates state common law and statutory law. Microsoft and the public will continue to be irreparably harmed if the Citadel Botnets continue to operate through the Harmful Domains and IP Addresses.

At the same time, if the TRO, seizure order and preliminary injunction is issued, no legitimate interests of Defendants will be harmed, and the effect on third-parties (domain registries and IP address hosting companies from whom Defendants acquired the Harmful Domains and IP Addresses and end-user victims) will be negligible and short lived. The public interest also weighs heavily in favor of relief because the same injury inflicted on Microsoft and its customers by the Citadel Botnets is also visited on the public at large. Accordingly, the relief Microsoft requests is warranted.

1. **Microsoft Is Likelv To Succeed On The Merits Of Its Claims**

Microsoft is likely to succeed on the merits of its claims and as such, its request for a TRO and a preliminary injunction should be granted. Microsoft's Complaint sets forth the following statutory and state common law and statutory claims: (1) violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030), (2) violations of the CAN-SPAM Act (15 U.S.C. § 7704), (3) violations of the Electronic Communications Privacy Act (18 U.S.C. § 2701); (4) trademark infringement under the Lanham Act (15 U.S.C. § 1114); (5) false designation of origin under the Lanham Act (15 U.S.C. § 1125(a)); (6) trademark dilution under the Lanham Act (15 U.S.C. 1125(c)), (7) violations of the Racketeer Influenced and Corrupt Organizations

Act; (8) computer trespass, (9) conversion, (10) unjust enrichment; and (11) nuisance.

a. Defendants' Computer Fraud And Abuse Act Violations

The Computer Fraud and Abuse Act ("CFAA") penalizes, *inter alia*, a party that:

- intentionally accesses a protected computer[1] without authorization, and as a result of such conduct, causes damage (18 U.S.C. § 1030(a)(5)(C)); or
- intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer (18 U.S.C. § 1030(a)(2)(C)); or
- knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer (18 U.S.C. § 1030(a)(5)(A)).

The servers of Microsoft and its Windows operating system running on computers are "protected computers" under the CFAA. Defendants intentionally access Microsoft's proprietary operating system and Microsoft's customers' computers, without authorization, and burden those computers by infecting them with malicious code and executing that code without consent. The Citadel Botnets intentionally access without authorization Microsoft's email servers (to send huge volumes of unsolicited, malicious spam email to Microsoft's customers). The Citadel Botnets intentionally access without authorization the servers of third-parties, including financial institution members, in order to access financial accounts and steal funds from these institutions and victim computer users.

The Citadel Botnets' intentional unauthorized access of Microsoft's protected computers, moreover, has resulted in substantial damages and loss, including the costs associated with investigating the unauthorized access. The evidence submitted in support of this motion demonstrates that Microsoft and its customers are damaged by this unauthorized

[1] A "protected computer" is a computer "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communications in the United States." 18 U.S.C. § 1030(e)(2)(B).

intrusion. Performance and operation of victim computers and Microsoft's software is degraded by the Citadel Botnets' intrusion. *See* Patel Decl. ¶¶69-76. Microsoft's email servers are burdened by the sending of an enormous amount of spam email. *Id.* ¶33. Microsoft and other members of the public must invest considerable time and resources investigating and remediating the Defendants' intrusion into these computers. *Id.* ¶ 76. Microsoft must spend time and resources to combat and remediate infections of user computers caused by the Citadel Botnets. *Id.* ¶ 76.

The Citadel Botnets' unauthorized access is precisely the type of activity the Computer Fraud and Abuse Act is designed to prevent. *See e.g. WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012) (CFAA is "designed to combat hacking"); *Big Rock Sports LLC v. Acusport Corp.*, 2011 U.S. Dist. LEXIS 110995, *4 (E.D.N.C. 2011) ("The CFAA penalizes 'access' or intrusions to a computer system…"); *Global Policy Partners, LLC v. Yessin,* 2009 U.S. Dist. LEXIS 112472, *9-13 (E.D. Va. 2009) (accessing computer using credentials that did not belong to defendant was actionable under the CFAA); *Physicians Interactive v. Lathian Sys., Inc.,* 2003 U.S. Dist. LEXIS 22868, *25 (E.D. Va. 2003) (granting TRO and preliminary injunction under CFAA where the defendant hacked into a computer and stole confidential information); *America Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 451 (E.D. Va. 1998) (defendant's unauthorized access of plaintiff's servers violated CFAA); *Facebook, Inc. v. Fisher*, 2009 U.S. Dist. LEXIS 122578 (N.D. Cal. 2009) (granting a TRO under CFAA where defendants allegedly engaged in a phishing (stealing sensitive information by masquerading as a reliable source) and spamming scheme that compromised the accounts of

Facebook users).[2] Accordingly, Microsoft is likely to succeed on the merits of its Computer Fraud and Abuse Act claim.

b. Defendants' CAN-SPAM Act Violations

The CAN-SPAM Act prohibits, among other acts, the initiation of a transmission of a commercial electronic mail message "that contains, or is accompanied by, header information that is materially false or materially misleading." 15 U.S.C. § 7704(a)(1). Defendants, through the botnet infrastructure, send e-mails containing false "header" information (*i.e.* originating sender, IP address, etc.) making the e-mails appear to originate from addresses purporting to be associated with Microsoft, or third party financial institutions, NACHA and other companies, or other false addresses, thereby disguising their origin with the purpose of misleading recipients and evading detection. *See* Sections I.C.3, *supra* pp. 12-13 and I.F.2, *supra* p. 21. This is precisely what CAN-SPAM prohibits. *See Aitken v. Communs. Workers of Am.*, 496 F. Supp. 2d 653, 667 (E.D. Va. 2007) (inaccurate "from" line and header information may violate CAN-SPAM); *Yahoo! Inc. v. XYZ Cos.*, 2011 WL 6072263, *4 (S.D.N.Y. Dec. 5, 2011) (holding that the transmission of numerous commercial emails with subject headings that misleads recipients into believing the "Lottery Fraud" emails were authorized by plaintiff and were sent through the plaintiffs servers would violate the CAN-SPAM Act). Microsoft is therefore likely to succeed on the merits of its CAN-SPAM Act claim.

c. Defendants' Electronic Communications Privacy Act Violations

The Electronic Communications Privacy Act prohibits "intentionally access[ing] without

[2] Indeed, in recent years botnet operators who disseminate code that intrudes upon user computers, collects personal information and causes injury have been indicted and convicted criminally under the Computer Fraud & Abuse Act. *See* Cox Decl. ¶¶ 36-37, Exs. 10 (Indictment of Jeanson James Ancheta), 37 (Sentencing of Jeanson James Ancheta).

authorization a facility through which electronic communications are provided" or doing so in excess of authorization and, in doing so, obtaining, altering, or preventing authorized access to an electronic communication while it is in electronic storage. 18 U.S.C. § 2701(a). Microsoft's licensed Windows operating system on end-user computers and servers of third-party financial institutions are facilities through which electronic communication services are provided. The Citadel Botnets' malicious code, installed without authorization on infected computers, searches emails and other files, intercepts user communications to and from websites, steals the contents of those communications stored on computers, and steals end-user's banking credentials and other information. Once harvested, the stolen credentials are used to steal personal information and money or to send spam email from compromised email accounts. Obtaining stored electronic information in this way, without authorization, is a violation of the Electronic Communications Privacy Act. *See Global Policy Partners, LLC*, 2009 U.S. Dist. LEXIS 112472 at *9-13 (unauthorized access to emails was actionable under ECPA); *State Analysis, Inc. v. American Fin. Srvcs. Assoc.*, 621 F. Supp. 2d 309, 317-18 (E.D. Va. 2009) (access of data on a computer without authorization actionable under ECPA); *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC,* 759 F. Supp. 2d 417 (S.D.N.Y. 2010) (unauthorized access of emails stored on a third-party communication service provider system violated the ECPA), *cited with approval Bryan v. Bryan*, 2012 U.S. Dist. LEXIS 150648, *1-2 (W.D.N.C. 2012).

d. Defendants' Lanham Act Violations

Section 1114(1) of the Lanham Act prohibits use of a reproduction, counterfeit, copy or "colorable imitation" of a registered mark in connection with the distribution of goods and services where such use is likely to cause confusion or mistake or to deceive. Defendants distribute copies of Microsoft's registered, famous and distinctive trademarks in fraudulent versions of its Windows operating system and Internet Explorer browser, which deceive victims, causing them confusion and causing them to mistakenly associate Microsoft with this activity. Defendants similarly misuse the trademarks of third party financial institutions, NACHA and other institutions as well. *See* Sections I.C.3, *supra* pp. 12-13 and I.F.2, *supra* p. 21.

The Citadel Botnet also makes such use of trademarks in website templates and spam templates that Defendants then use to mislead Internet users into providing their credentials. Defendants steal those credentials and use them to raid Internet users' financial accounts. Defendants' creation and use of counterfeit trademarks in connection with such severe fraud is likely to cause confusion and mistake and to deceive consumers. This is a clear violation of the Lanham Act and Microsoft is likely to succeed on the merits. *See American Angus Ass'n v. Sysco Corp.*, 829 F. Supp. 807, 820 (W.D.N.C. 1992) (granting preliminary injunction where defendant's use of mark was likely to cause confusion); *IHOP Corp. v. Langley*, 2008 U.S. Dist. LEXIS 112056, *1-3 (E.D.N.C. 2008) (granting TRO where defendant's use of mark was likely to cause confusion); *Audi AG v. Shokan Coachworks, Inc.,* 592 F. Supp. 2d 246, 279 (N.D.N.Y. 2008) (holding that the use of the plaintiffs' marks in the defendants' email addresses created a likelihood of consumer confusion); *Brookfield Commc'ns. v. W. Coast Entm't Corp.*, 174 F.3d 1036, 1066-1067 (9th Cir. 1999) (entering preliminary injunction under Lanham Act §1114 for infringement of trademark in software and website code).

The Lanham Act also prohibits use of a trademark, any false designation of origin, false designation of fact or misleading representation of fact which:

> is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person.

15 U.S.C. § 1125(a). The Citadel Botnets' misleading and false uses of Microsoft's

trademarks—including "Microsoft," "Windows," "Internet Explorer"—and also the trademarks of third parties including "NACHA," the NACHA logo, "Bank of America," "Wells Fargo," "Citibank," and others, causing confusion and mistake as to affiliation with the malicious conduct carried out by the botnet. *See* Sections I.C.3, *supra* pp. 12-13 and I.F.2, *supra* p. 21. This activity is a clear violation of Lanham Act § 1125(a) and Microsoft is likely to succeed on the merits. *See Garden & Gun, LLC v. Twodalgals, LLC*, 2008 U.S. Dist. LEXIS 79982 (W.D.N.C. 2008) (granting preliminary injunction against misleading use of trademarks under Section 1125(a)); *IHOP Corp.*, 2008 U.S. Dist. LEXIS 112056 at *1-3 (same; granting TRO); *Am. Online v. IMS*, 24 F. Supp. 2d 548, 551-552 (E.D. Va. 1998) (misuse of trademark in e-mail headers violated §1125(a); also constituted trademark "dilution" under §1125(c)); *Brookfield Commc'ns.*, 174 F. 3d at 1066-67 (entering preliminary injunction under Lanham Act §1125(a) for infringement of trademark in software and website code); *Hotmail Corp. v. Van$ Money Pie, Inc.*, 1998 U.S. Dist. LEXIS 10729, *12-13 (N.D. Cal. 1998) (granting preliminary injunction; copying the Hotmail trademarks in "e-mail return addresses" constituted false designation of origin; also constituted trademark "dilution" under §1125(c)).

e. <u>Computer Trespass /Conversion</u>

A trespass to chattels occurs where a defendant interferes, unlawfully and without authorization, or dispossesses the personal property in the plaintiff's possession. *Fordham v. Eason*, 351 N.C. 151, 155 (1999). In particular, prohibitions on "Computer Trespass" have been enacted by statute at North Carolina General Statutes § 14-458. This provision prohibits, among other things, a defendant, without authority, from using a computer to "alter… computer programs, or computer software" or "to cause physical injury to the property of another" and defines such as a trespass. N.C. Gen. Stat. § 14-458(a)(3), (4). Similarly, conversion occurs where a defendant makes an unauthorized assumption and exercise of the right of ownership over goods belonging to another, to the alteration of their condition or the exclusion of the owner's rights. *Peed v. Burleson's, Inc.*, 244 N.C. 437, 439 (1956).

Defendants have intruded upon, interfered with and taken as their own Microsoft's resources and property, by (1) altering, interfering with, installing software within and causing injury to Microsoft's licensed Windows operating system on victim computers and (2) interfering with and intruding upon Microsoft's Hotmail servers to which Defendants send vast quantities of spam e-mail. These activities injure the value of Microsoft's property and constitute a trespass and conversion. *See* N.C. Gen. Stat. § 14-458(a)(3), (4); *Bridgetree, Inc. v. Red F Mktg. LLC*, 2013 U.S. Dist. LEXIS 15372, *45-51 (W.D.N.C. 2013) (defendants liable under North Carolina law for conversion of computer files where they were not authorized to own the files and excluded the owner from exercising right of ownership and control over them); *Springs v. Mayer Brown, LLP*, 2012 U.S. Dist. LEXIS 9734 (W.D.N.C. 2012) (under North Carolina law, conversion could be predicated on taking a copy of a computer file, as it deprived plaintiff from control over its property); *see also Kremen v. Cohen*, 337 F.3d 1024, 1034 (9th Cir. 2003) (hacking into computer system and injuring data supports a conversion claim); *Physicians Interactive v. Lathian Sys.*, 2003 U.S. Dist. LEXIS 22868, at *25, 31 (E.D. Va. 2003) (TRO and preliminary injunction where defendant hacked computers and obtained proprietary information).

f. **<u>Unjust Enrichment</u>**

The elements of a claim of unjust enrichment are that a (1) defendant benefitted, (2) the benefit was not gratuitous, (3) the benefit is measurable, and (4) the defendant consciously accepted the benefit. *Carty v. Westport Homes of N.C., Inc.*, 472 Fed. Appx. 255, 258-9 (4th Cir. 2012) (citing *Booe v. Shadrick*, 322 N.C. 567, 570 (1988)). Defendants controlling the Citadel Botnets have benefited from Microsoft's Windows operating system, Internet Explorer browser, and servers as well as its trademarks, brand names, and goodwill by, among other things, intruding upon and converting for their own use Microsoft's property, to further Defendants' banking fraud on users of Microsoft's Windows operating system. *See* Sections I.C.3, *supra* p. 13 and I.F.1, *supra* p. 21. Defendants have specifically taken, without authorization, the benefit of Microsoft's software in order to steal information and money. In each instance, Defendants have profited from their unlawful activity, reaping millions of dollars in stolen money and information. Thus, it is certainly inequitable for Defendants controlling the Citadel Botnets to retain these benefits. Accordingly, Microsoft is likely to succeed on the merits.

g. **Nuisance**

"[A] private nuisance exists in a legal sense when one makes an improper use of his own property and in that way injures the land or some incorporeal right of one's neighbor." *Morgan v. High Penn Oil Co.*, 238 N.C. 185, 193 (1953) (citations omitted); *Evans v. Lochmere Rec. Club*, 176 N.C. App. 724, 727-728 (N.C. Ct. App. 2006) (stating claim for nuisance where defendant "has used amplified sound from speakers aimed directly at [plaintiffs'] premises"). A private nuisance action may arise from the defendant's intentional and unreasonable conduct or it may be grounded in negligence. *Pendergrast v. Aiken*, 293 N.C. 201, 236 S.E. 2d 787 (1977); Restatement (Second) of Torts Sec. 822 (1979).

Here, Defendants operating software on victim computers have intentionally directed their malicious activities and misused their property and the property of others, in a manner that injures the rights of Microsoft. Defendants' conduct is highly unreasonable, has no social value and thus constitutes a nuisance, which should be abated by the injunctive relief sought herein. *See Mayes v. Tabor*, 77 N.C. App. 197, 199-201 (N.C. Ct. App. 1985) (error to deny injunction to abate a nuisance).

h. **Defendants' Racketeer Influenced and Corrupt Organizations Act (RICO) Violations**

The Racketeer Influenced and Corrupt Organizations Act ("RICO") prohibits "any person employed by or associated with any enterprise engaged in, or the activities of which affect, interstate or foreign commerce to conduct or participate, directly or indirectly, in the conduct of such enterprise's affairs through a pattern of racketeering activity." 18 U.S.C. § 1962(c). RICO also makes it unlawful "for any person to conspire to violate" that provision, regardless of whether that conspiracy ultimately comes to fruition. 18 U.S.C. §1962(d). "Any person injured in his business or property by reason of a violation of" either of these provisions is entitled to recovery, 18 U.S.C. § 1964(c), and this court has "jurisdiction to prevent and restrain" such violations "by issuing appropriate orders." 18 U.S.C. 1964(a).

Defendants in this case have formed and associated with such an enterprise affecting foreign and interstate commerce and have engaged in an unlawful pattern of racketeering activity involving thousands of predicate acts of "access device" fraud, 18 U.S.C. § 1029, as well as wire fraud, 18 U.S.C. § 1343 and bank fraud, 18 U.S.C. § 1344.

(1) **The Citadel Enterprise**

An associated in fact enterprise consists of "a group of persons associated together for a common purpose of engaging in a course of conduct" and "is proved by evidence of an ongoing organization, formal or informal, and by evidence that the various associates function as a continuing unit." *Boyle v. United States*, 556 U.S. 938, 945 (2009). An enterprise requires "at least three structural features: a purpose, relationships among those associated with the enterprise, and longevity sufficient to permit these associates to pursue the enterprise's purpose." (*Id.*)

The Citadel Enterprise has existed since at least January 2012, when John Doe 1 began offering the Citadel botnet kit to John Does 2-82. *See* Patel Decl. ¶¶82-89. John Does 2-82 joined and began participating in the Citadel Enterprise at various times thereafter. Patel Decl. ¶¶90-96. *See United States v. Banks*, 10 F.3d 1044, 1053-54 (4th Cir. 1993) (single conspiracy found even where loose organizational structure, changing membership, shifting roles of participants, limited roles and knowledge of some members). The Citadel Enterprise has continuously and effectively carried out its purpose of developing and operating global credential stealing botnets ever since, and will continue to do so absent the relief Microsoft requests. *See* Patel Decl. ¶¶ 97-98.

Defendants' interrelated roles in the operation of the Citadel Botnets, in furtherance of common financial interests, demonstrate the purpose of the Citadel Enterprise and the relationship between the Defendants. *Boyle*, 556 U.S. at 945 (relationship and common interest may be inferred from "evidence used to prove the pattern of racketeering activity"). The relationship between Defendants may also be inferred by the Defendants' development and/or purchasing of the Citadel botnet code and their use of the Citadel botnet system to steal and exploit credentials and money. *See* Patel Decl. ¶¶81-87, 97-98.

(2) <u>Defendants' Pattern of Racketeering Activity</u>

A pattern of racketeering activity "requires at least two acts of racketeering activity, one of which occurred after [October 15, 1970,] and the last of which occurred within ten years . . . after the commission of a prior act of racketeering activity." *H.J. Inc. v. Northwestern Bell Tel. Co.*, 492 U.S. 229, 237 (1989). The threat of continuity of interrelated acts may be inferred from "past conduct that by its nature projects into the future with a threat of repetition." *H.J. Inc.* at 241; *Eplus Tech., Inc. v. Aboud*, 313 F.3d 166, 181-182 (4th Cir. Va. 2002). Defendants have conspired to, and have, conducted and participated in the operations of the Citadel Enterprise through a continuous pattern of racketeering activity. Each predicate act is related and in furtherance of the common unlawful purpose shared by the members of the Citadel Enterprise. These acts are continuing and will continue unless and until this Court grants Microsoft's request for a temporary restraining order.

Defendants' acts of racketeering activity include access device fraud, in violation of 18 U.S.C. § 1029. Whoever "knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices" or "knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that that period," is guilty of violating 18 U.S.C. § 1029 "if the offense affects interstate or foreign commerce." 18 U.S.C. §1029(a)(1) & (2). An "access device" includes "any. . . code, account number, electronic serial number, mobile identification number [or] personal identification number. . . that can be used, alone or in conjunction with another access device, to obtain money. . . or any other thing of value, or that can be used to initiate a transfer of funds." 18 U.S.C. §1029(e)(1). An "unauthorized access device" includes "any access device that is lost, stolen . . . or obtained with intent to defraud." 18 U.S.C. §1029(e)(3). Violation of this statute constitutes "racketeering activity." 18 U.S.C. §1961(1)(B).

Defendants have conspired to, and have, knowingly and with intent to defraud used an unauthorized access device in the form of an unauthorized Windows XP product key to install a stolen copy of Windows XP in order to produce the necessary Citadel botnet software operated by Defendants. *See* Patel Decl. ¶¶7, 27-28; Krumm Decl. ¶¶6, 7. A product key is an authorization code used to "unlock" and gain access to Microsoft Windows, or other software, and thus grants users access to the valuable services provided by the software. *See* Krumm Decl. ¶¶2-5. Such an authorization code can be considered an "access device" under 18 U.S.C. §

1029(e)(1). *See United States v. Brewer*, 835 F.2d 550, 553 (5th Cir. 1987) (finding access codes used to access a phone system to make long distance calls to be an "access device" under 18 U.S.C. § 1029(e)(1)); *accord United States v. Barrington*, 648 F.3d 1178, 1201 n.23 (11th Cir. 2011) ("[W]e have broadly constructed the definition of access device to include 'innovative means that parties use to gain unauthorized information to engage in fraudulent activities.'"). Further, an authorization code can be considered "counterfeit" or "unauthorized" even if it is accepted by the software as legitimate. *See Brewer*, 835 F.2d at 554 (finding that a code could be counterfeit even if they were legitimately accepted in the same way that a fake credit card is no less counterfeit just because it happens to match a valid account).

Congressional intent indicates that the term "access device" should be broadly construed to accommodate technological changes and advances. *See Brewer*, 835 F.2d at 553 n.1 (citing S. Rep. No. 98-368, 98th Cong., 2d Sess., *reprinted in* 1984 U.S. Code Cong. & Ad. News 3182, 3647, at 3655; H.R. Rep. No. 98-894, 98th Cong., 2d Sess., *reprinted in* 1984 U.S. Code Cong. & Ad. News 3689, at 3705) (noting that the legislative history of § 1029 indicates that Congress wanted the statute to be "broad enough to encompass technological advances."); *see also United States v. Ashe*, 47 F.3d 770, 774 (6th Cir. 1995) (holding that "invasion of an identifiable customer's account is not a necessary element of proof"); *United States v. Bailey*, 41 F.3d 413, 418 (9th Cir. 1994) (holding that nowhere in § 1029 does it "impl[y] that the only 'account' protected against improper access is one maintained by an end consumer.").

As set forth in detail above, Defendants provide a stolen copy of Windows XP as well as an unauthorized product key to provide access to said copy of Windows XP in the Citadel manual to all members of the Citadel Enterprise so that the members can use this copy to build and produce the Citadel botnet software. *See* Patel Decl. ¶¶7, 27-28. Defendants then use the

Citadel botnet software, built upon this stolen copy of Windows XP and unauthorized key, to access financial accounts.

Furthermore, Defendants have also conspired to, and have, knowingly and with intent to defraud trafficked in thousands of unauthorized access devices in the form of stolen passwords, bank account numbers and other account login credentials through the Citadel botnet system created and operated by Defendants. *See* Patel Decl. ¶¶10, 56-57. As set forth in detail above, Defendants have used the Citadel botnet system to intrude upon the computers and software of Microsoft and its customers, then steal, intercept and obtain this access device information from thousands of individuals using falsified web pages, and have then used these fraudulently obtained unauthorized access devices to steal millions of dollars from these individuals' accounts, in violation of 18 U.S.C. § 1029(a)(2).[3] Each of these illegal acts was conducted using interstate and/or foreign wires, and therefore affected interstate and/or foreign commerce.[4]

(3) Microsoft's Injury as a Direct Result of Defendants' Pattern of Racketeering Activity

Defendants' Botnets have carried out such massive theft by infecting millions of computers running Microsoft's Windows operating system with its malicious software and flooded millions of email accounts, including Microsoft Hotmail email accounts, with spam

[3] Defendants' conduct also constitutes access device fraud under 18 U.S.C. §1029(a)(3) (possession of unauthorized access devices) and 18 U.S.C. §1029(a)(7) (effecting transactions with unauthorized access devices).

[4] Defendants' conduct is also "racketeering activity" in the form of bank fraud under 18 U.S.C. § 1344 (violation where one "knowingly executes, or attempts to execute, a scheme or artifice (1) to defraud a financial institution; or (2) to obtain any of the moneys, funds, credits, assets, securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations, or promises"), and wire fraud under 18 U.S.C. § 1343 (violation where one "having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire. . . communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice.").

messages infringing trademarks, and containing links designed to infect computers with malicious software and steal credentials. As a direct result of Defendants' conduct, Microsoft has been forced to spend resources to mitigate the impact to its customers, and investigate the source of the Citadel botnet and the online identities of Defendants and other members of the Citadel Enterprise. Patel Decl. ¶76. Accordingly, there is a "direct relation between the injury asserted and the injurious conduct alleged" *Hemi Group, LLC v. City of New York*, 130 S. Ct. 983, 989 (U.S. 2010).[5]

2. Irreparable Harm Will Result Unless a TRO and Preliminary Injunction Are Granted

Continued operation of the Citadel Botnets irreparably harms Microsoft, its customers and the general public. No monetary remedy could repair the harm if the Citadel Botnets were permitted to continue operating and expanding. Federal courts addressing botnets have concluded that the "immediate and irreparable harm" to consumers from "botnet command and control servers, spyware, viruses, Trojans, and phishing-related sites; and configuring, deploying and operating botnets," warranted an *ex parte* TRO and preliminary injunction. *See* Cox Decl., Exs. 16, 17 (*Microsoft Corp. v. Piatti, et al.*, Case No. 1:11-cv-1017 (E.D. Va., Cacheris, J.)); Exs. 14, 15 (*Microsoft Corp. v. John Does 1-11*, Case No. 2:11-cv-00222 (W.D. Wash. 2011, Robart, J.)); Exs. 12, 13, (*Microsoft Corp. v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va., Brinkema J.)); Exs. 8, 9 (*FTC v. Pricewert LLC et al.*, Case No. 09-2407 (N.D. Cal., Whyte J)). These courts have acknowledged the substantial irreparable harm botnets cause Microsoft, its customers and Internet users generally.

Microsoft, its customers, and the public face the same irreparable harm caused by the

[5] Where the pattern of racketeering activity consists of fraud, as here, a plaintiff need not show that it relied on or was deceived by the defendant's fraud – third party reliance is sufficient. *Id.*, *quoting Bridge v. Phoenix Bond & Indem. Co.*, 553 U.S. 639, 657-58 (2008).

Citadel Botnets. Thus, entry of an *ex parte* TRO redirecting the Harmful Domains and IP Addresses to secure computers, thus disabling them and preserving evidence of Defendants' misconduct and injury to victims, and an Order to Show Cause why a preliminary injunction should not issue, is warranted. Microsoft is irreparably injured because of the problems described above. Customers of Microsoft may migrate to other platforms, products or services in the mistaken belief that Microsoft is the cause of the problems. Customers may cease conducting online transactions. Once such a switch occurs, given the costs of switching platforms and the uncertainty caused by the botnet in the first place, there is a very high risk that those customers will not return to Microsoft or to carry out online transactions

Further, given Defendants' very visible fraud involving infringement of Microsoft's trademarks, Microsoft is irreparably injured because the problems created by the Citadel Botnets are improperly attributed to Microsoft. *See* Sections I.C.3, *supra* pp. 12-13 and I.F.1, *supra* p. 21. The Defendants' unauthorized use of trademarks in order to deceive consumers and to carry out identity theft and bank fraud diminishes the brands and goodwill of Microsoft. This causes confusion to consumers, leaving them to attribute the harm to Microsoft.

As the Citadel Botnets continue to grow, this harm is compounded. This type of brand related injury and customer harm is most certainly irreparable and is precisely why the relief requested in this motion should be granted. *See Blackwelder Furniture Co. v. Seilig Mfg. Co.*, 550 F.2d 189, 197 (4th Cir. 1977) (finding loss of goodwill as irreparable harm), *overruled on other grounds, The Real Truth About Obama, Inc. v. FEC*, 575 F.3d 342, 347 (4th Cir. 2009); *see also Tom Doherty Assocs., Inc. v. Saban Entm't, Inc.,* 60 F.3d 27, 37-38 (2d Cir. 1995) (recognizing that the loss of prospective business or goodwill supports a finding of irreparable harm).

Further, if the requested relief were not granted, the computers of Microsoft's customers would continue to be infected and the Citadel Botnets would grow. This injury is irreparable because customers and the general public, for the most part, lack the technical knowledge, skills, and ability to remedy the infection or curtail the growth of the Citadel Botnets. In the absence of the requested relief, Microsoft's customers and the general public would remain under constant threat of their computers being made part of the botnet with the accompanying harmful effects of unauthorized intrusion into and abuse of their computers.

3. The Balance Of Hardships Tips Sharply In Microsoft's Favor

Defendants will suffer *no harm* to any legitimate interest if an *ex parte* TRO and preliminary injunction are issued, because it will do no more than preserve the status quo and ameliorate the negative effects of the botnets. Redirecting the Harmful Domains and IP Addresses to secure computers will prevent the Citadel Botnets from spreading to any additional computers during that time, and will preserve the evidence of the botnet's structure and illegal activities and evidence of the injury to victims. Microsoft has identified no legitimate activities carried on from and through these domains and IP addresses. They serve solely to support the Citadel Botnets. Similarly, there will be only negligible impact on the third-party domain registries and hosting companies whose services Defendants are using and the victim end-users whose computers will be protected, as the requested relief is carefully tailored to only redirect or disable domains and IP addresses supporting the botnet, directs these third parties to take simple steps, part of their normal operations, to redirect or disable this infrastructure and assist in preserving evidence and directs limited steps to disable the botnet capabilities in victim computers and notify those victims of steps they can take to protect themselves.

Conversely, if a TRO and preliminary injunction do not issue, the Citadel Botnets will continue to inflict irreparable injury on Microsoft, its customers and the public. The Citadel Botnets are already responsible for millions of dollars stolen from many financial institutions. New users are infected each day, dramatically increasing the Citadel Botnets' capacity to carry out illegal conduct, compounding the injury to Microsoft, its customers and the public.

Simply put, maintaining the status quo by disabling the Harmful Domains and IP Addresses through which the Citadel Botnets are controlled, disabling the botnets' capabilities in victim computers and notifying those victims will not affect any legitimate rights of Defendants or third parties. Microsoft seeks tailored assistance from the third-party domain registries and hosting companies and limited steps to disable the botnets and notify victims. However, allowing the Citadel Botnets to grow and continue to harm Microsoft, its customers and the public while this action is adjudicated poses grave danger to many legitimate interests.

4. **The Public Interest Will Be Served By The Issuance Of A TRO And Preliminary Injunction**

A TRO and preliminary injunction protects the public interest and not just Microsoft and its customers because the Citadel Botnets' bank fraud poses serious financial threats to individual consumers and the financial industry. The Citadel Botnets, moreover, target government agencies and websites all over the world. Every website provider, financial institution, government agency, and consumer with access to the Internet or an e-mail platform and the Internet is at risk of being irreparably injured by the Citadel Botnets.

There is an overwhelming public interest in preserving the status quo and halting the growth of the Citadel Botnets while Microsoft proceeds with its claims. Three district courts have concluded on six occasions in the last three years that "immediate and irreparable harm" will result to the welfare of consumers from "botnet command and control servers" and the malicious conduct carried out through botnets. Cox Decl., Exs. 12-21. Likewise, a TRO and preliminary injunction here will preserve and protect this important public interest. No such protection will be afforded if preliminary relief is denied and, in that event, the malicious actors controlling the Citadel Botnets will be able to continue their activities with impunity.

5. **Only The Requested *Ex Parte* Relief Can Halt The Irreparable Harm To Microsoft And The Public**

Absent a TRO granting the relief requested herein, the injury to Microsoft, its customers and the public will continue unabated, irreparably harming Microsoft's reputation, brand and goodwill. The TRO, moreover, must issue *ex parte* for the relief to be effective at all, and the extraordinary factual circumstances here warrant such relief. Rule 65 of the Federal Rules of Civil Procedure permits an *ex parte* TRO where the moving party sets forth facts that show an immediate and irreparable injury and why notice should not be required. Fed. R. Civ. P. 65(b)(1); *see Granny Goose Foods, Inc. v. Teamsters,* 415 U.S. 423, 438-39 (1974) ("*Ex parte* temporary restraining orders are no doubt necessary in certain circumstances. . . .").

a. **If Notice Is Given, The Botnet Will Be Moved And Concealed, Allowing The Harm To Grow And Render Microsoft's Request For Relief Fruitless**

If notice is given prior to issuance of a TRO, the Citadel Botnets' command and control infrastructure operating through the Harmful Domains and IP Addresses will be moved to different servers, at different domains and IP addresses, in different areas, enabling Defendants controlling the Citadel Botnets to continue infecting users' computers with malicious software and carrying out the malicious activities described above. Indeed, there is specific evidence that Defendants have evaded prior enforcement attempts, where they had notice, by moving the command and control infrastructure. *See* Patel Decl. ¶¶99-105. If Defendants are allowed to do so here, the investigation of the botnet and the illicit activities carried out through it would have to be started anew. *Id.* Providing notice of the requested TRO will undoubtedly facilitate efforts of the Defendants to evade enforcement efforts.

It is well-established that *ex parte* relief is appropriate under circumstances such as the instant case, where notice would render the requested relief "fruitless." *See e.g. Christian Louboutin S.A. v. Chantarungsri*, 2009 U.S. Dist. LEXIS 131720, *4-5 (E.D.N.C. 2009) (granting *ex parte* TRO where it was shown that "defendants may take action to transfer their assets and thus avoid an accounting of defendants' profits from their unlawful activities."); *In re Vuitton Et Fils S.A.*, 606 F.2d 1, 4 (2d Cir. 1979) (*per curiam*) (holding that notice prior to issuing TRO was not necessary where notice would "serve only to render fruitless further prosecution of the action"; prior experience taught that once one member of the counterfeiting enterprise received notice, contraband would be transferred to another unknown counterfeiter, perpetuating the harm and rendering judicial efforts pointless); *Allscripts Misys, LLC v. Am. Digital Networks, LLC*, 2010 U.S. Dist. LEXIS 4450, *2 (D. Md. 2010) (granting an *ex parte* TRO where "Defendant may dissipate the funds and/or take action to render it difficult to recover funds....")

Where there is specific evidence that botnets operators have attempted to and will attempt to evade enforcement attempts when given notice, by moving the command and control infrastructure, courts have repeatedly granted such *ex parte* relief. *See* Cox Decl., Exs. 12-21 (*Microsoft Corp.,* Case No. 1:10-cv-156 (LMB/JFA) (E.D. Va., Brinkema J.); *Microsoft Corp. v. John Does, 1-11,* Case No. 2:11cv-00222 (W.D. Wash. 2011) (Robart, J.); *Microsoft Corp. v. Dominique Alexander Piatti, et al.*, Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.); *Microsoft Corp. v. Peng Yong et al.*, Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.); *Microsoft Corp. v. John Does 1-18*, Case No: 1:13-cv-139 (E.D. Va. 2013, Brinkema, J.).

Also instructive is *FTC v. Pricewert LLC et al.,* where the court issued an *ex parte* TRO suspending Internet connectivity of a company enabling botnet activity and other illegal computer-related conduct on the basis that "[the] Defendant is likely to relocate the harmful and malicious code it hosts and/or warn its criminal clientele of this action if informed of the [plaintiff's] action." *See* Cox Decl., Ex. 8-9 (*FTC v. Pricewert LLC et al.*, Case No. 09-2407 (N.D. Cal., Whyte J.).) Moreover, the court in *Dell, Inc. v. Belgiumdomains, LLC,* 2007 U.S. Dist. LEXIS 98676, *4-5 (S.D. Fla. Nov. 21, 2007) issued an *ex parte* TRO against domain registrants where persons similarly situated had previously concealed such conduct and disregarded court orders by, *inter alia*, using fictitious businesses, personal names, and shell entities to hide their activities. *Id.* at *4. In *Dell*, the Court explicitly found that where, as in the instant case, Defendants' scheme is "in electronic form and subject to quick, easy, untraceable destruction by Defendants," ex parte relief is particularly warranted. *Id.* at *5-6.

b. **If Notice Is Given, Evidence Regarding The Citadel Botnets Will Be Destroyed, Disturbing The Status Quo**

If notice is given in advance, evidence of the botnet will be destroyed. In particular, upon notice, the movement of the botnet command and control software will destroy both evidence of the botnet's operation and the injury caused by the botnets. Under such circumstances, courts have issued *ex parte* TROs. *See e.g. Christian Louboutin S.A. v. Chantarungsri*, 2009 U.S. Dist. LEXIS 131720, *4-5 (E.D.N.C. 2009) (granting *ex parte* TRO where it was shown that defendants "would likely destroy, move, hide or otherwise make inaccessible" evidence of misconduct); *AT&T Broadband v. Tech Commc'ns, Inc.* 381 F.3d 1309, 1319-1320 (11th Cir. 2004) (affirming *ex parte* search and seizure order to seize contraband technical equipment, given evidence that in the past defendants and persons similarly situated had secreted evidence once notice given); *Dell, Inc,* 2007 U.S. Dist. LEXIS 98676 at *4-5; *Little Tor Auto Center v. Exxon Co., U.S.A.*, 822 F. Supp. 141, 143 (S.D.N.Y.

1993) (*ex parte* TRO appropriate where contraband "may be destroyed as soon as notice is given"). For this reason, the requested *ex parte* TRO is warranted.

B. <u>Only An *Ex Parte* Seizure Order Can Halt The Irreparable Harm To Microsoft And The Public</u>

The Citadel Botnets are specifically designed to resist technical mitigation efforts, eliminating viable technical means to curb the injury. Patel Decl. ¶¶45-51. The Citadel Botnets, moreover, are designed to destroy evidence and conceal their misconduct. *Id.* Coupled with Defendants' technological sophistication and expertise in evading enforcement, there is an overwhelming risk that if the most active, current command and control software hosted at the Harmful Domains and IP Addresses are not redirected to secure computers, thus disabling them, the botnet code on victim computers are not disabled via a specially crafted configuration file, and the Defendants' computers at the Harmful IP addresses seized with the assistance of the United States Marshals Service, Defendants will be able to move the Citadel Botnets, continue their trademark infringement and continue their related activities causing irreparable harm. Thus, the redirection of the Harmful Domains and IP Addresses of the most active, current command and control software to secure computers and the disabling of the harmful botnet code are warranted.

Section 1116(d) of the Lanham Act provides for *ex parte* seizure and impoundment of infringing and counterfeit items, the instrumentalities used to reproduce the infringing and counterfeit articles, and the records documenting the manufacture, sale and receipt of such materials. *See* 15 U.S.C. § 1116(d); *Christian Louboutin S.A. v. Chantarungsri*, 2009 U.S. Dist. LEXIS 131720, *4-5 (E.D.N.C. 2009) (granting *ex parte* TRO authorizing seizure of instrumentalities of trademark infringement under §1116(d)). It is well-established that an *ex parte* seizure order is appropriate where notice would allow defendants to continue their infringement or to destroy, move, hide or otherwise make inaccessible evidence of infringement. *See Microsoft Corp. v. Jun Yan*, 2010 U.S. dis. Lexis 14933 at *1; *AT&T Broadband,* 381 F.3d at 1319; *In re Vuitton Et Fils S.A.*, 606 F.2d at 4. It is also well-settled that courts can impound computers, servers and other electronic data that constitute infringing items, instrumentalities used to carry out infringement, or records of infringement. *See e.g., Dell,* 2007 U.S. Dist. LEXIS 98676 at *12-13 (issuing an *ex parte* TRO and seizure order under Section 1116(d) that allowed for a forensic analysis of the defendants' computer data for records).

The Lanham Act authorizes an *ex parte* seizure and impoundment order where the court (1) finds no order other than an *ex parte* seizure is adequate to achieve the purpose of Section 1114; (2) the applicant has not publicized the requested seizure; (3) the applicant is likely to succeed in showing the person against whom seizure would be ordered used the counterfeit mark in connection with the sale, offer for sale or distribution of goods or services; (4) the applicant will suffer irreparable harm; (5) the matter to be seized will be located at the place identified in the application; (6) the balance of hardships tip in favor of seizure; and (7) the persons against whom seizure would be ordered or those working in concert with them would destroy, move, hide or otherwise make such matter inaccessible to the court if the applicant provided notice. *See* 15 U.S.C. § 1116(d)(i)-(vii). Each of these criteria is met in this case.

1. Only Redirecting The Harmful Domains And IP Addresses To Secure Computers, Disabling the Botnet Code on Victim Computers And Seizing The Defendants' Servers At The Harmful IP Addresses Can Ensure That Defendants Will Not Continue Their Activities Or Destroy Or Conceal Evidence

An *ex parte* seizure order redirecting the domains and IP addresses of the most active command and control servers to secure computers is critical to ensure that Defendants cannot continue their deceptive use of Microsoft's trademarks and to ensure that Defendants will not destroy or conceal evidence, all of which would render the further prosecution of this action fruitless. Here, there is substantial evidence that if (1) the Harmful Domains and IP Addresses are not redirected to secure computers, (2) the botnet code is not disabled on Victim Computers, and (3) Defendants' servers at the Harmful IP Addresses are not physically seized in a highly coordinated manner, Defendants will be able to continue their misleading and illegal use of Microsoft's trademarks in unauthorized software on victim computers and spam e-mails.

The efficacy of such seizure orders against cyber criminals – like Defendants here – is best demonstrated by the Rustock botnet (the largest spam botnet at the time). In a previous enforcement attempt against the Rustock botnet, its operators were able to move the command and control infrastructure during a brief period when the Internet Service Provider inadvertently restored the connection to the domains and IP addresses the Rustock botnet used to communicate with the infected end-user computers. Cox Decl., ¶3. This allowed the Rustock botnet to continue harming Microsoft and the public for years through spam campaigns. By contrast, a subsequent order issued in a civil action by the District Court for the Western District of Washington, directing seizure of that botnet's command and control servers, resulted in cessation of the botnet's harmful activities.

In order to ensure the most effective and permanent disabling and dissolution of the Citadel Botnets, Defendants' malicious botnet code must be disabled on the victim computers and the victims must be notified. Microsoft customers agree to license terms for Microsoft's software, which permit Microsoft to remove malicious software, ensure that software is validated as secure and properly licensed, and to remedy and repair Microsoft software to ensure that it is secure and properly licensed, both to protect Microsoft's property interests in its licensed software and to ensure optimal user experience free from malicious and deleterious consequences, such as banking fraud software like the Citadel botnet. Patel Decl., Exs. 15 (Windows 7 license at ¶¶ 4-8), 16 (Windows Vista license at ¶¶ 4-8), 17 (Windows XP license at ¶¶1-2).

Such relief issuing parameters to disable botnet code has been ordered in prior civil actions addressing the threat of botnets. *See United States v. John Does 1-13*, Case No. 3:11-cv-561 (VLB) (D. Conn. 2011), at Cox Decl., Ex. 22 (Government's civil complaint to disable the "Coreflood" botnet), Ex. 23 at p. 3, 5-6 (preliminary injunction ordering "issuing instructions that will cause the [botnet] software on infected computers to stop running," finding that "allowing the [botnet software] to continue running on the infected computers will cause a continuing and substantial injury").

Such an order in this case is warranted to preserve the evidence, thwart Defendants' continued operation of the Citadel Botnets, protect victims and protect against inadvertent or intentional acts by any third party that would enable Defendants to continue their activities and/or destroy evidence of the operation of Citadel Botnets.

2. <u>Microsoft Will Not Publicize The Requested Seizure In Advance</u>

Other than notifying the Department of Justice in Washington, DC, the United States Attorney for the Western District Of North Carolina, and the United States Marshals Service in districts where seizure is to be effected and preparing for service of process after any order is executed, pursuant to Section 1116(d)(2) of the Lanham Act, Microsoft has not and will not publicize the requested seizure until after the requested seizure is carried out. Cox Decl. ¶13.

3. <u>Microsoft Is Likely To Succeed On The Merits Of Its Trademark Infringement Claim</u>

As discussed in detail above, the Citadel Botnets' command and control infrastructure hosted at the Harmful Domains and IP Addresses control unauthorized software that infringes

Microsoft's trademarks and contain trademark-infringing website and spam templates, including but not limited to those attached as Appendices A and B to the Complaint. This constitutes trademark infringement and false designation of origin under Sections 1114 and 1125(a) of the Lanham Act. The command and control infrastructure and software hosted at and operating through the Harmful Domains and IP Addresses both contain counterfeit trademarks and are instrumentalities used to carry out the infringement. Thus, Microsoft is likely to succeed on the merits and the command and control software is subject to seizure and impoundment under Section 1116(d) of the Lanham Act.

4. **Immediate And Irreparable Injury Will Occur If An *Ex Parte* Seizure Order Does Not Issue**

As discussed above Microsoft, its customers, and the public will continue to suffer irreparable harm if the Citadel Botnets are allowed to continue growing through the infringement of Microsoft's trademarks and are allowed to carry out their malicious activities.

5. **The Material To Be Seized And The Locations To Be Searched Are Identified In The Application**

In its proposed TRO and seizure order, Microsoft identifies with specificity the items to be seized and the places where Defendants' command and control infrastructure for the Citadel Botnets can be found. The proposed order identifies the following:

A. Appendix A to the proposed order identifies Defendants' specific harmful domains (domains such as cash-men.tf, fastspy.info, microsoft-ie-update.com, ylamixambistarimbasicolasta.com and others) and identifies the specific domain registries through which Defendants registered the domains. The domain registries are directed to redirect Defendants' Harmful Domains to specific IP addresses of secure computers, in order to disable those domains and preserve evidence available through them;

B. Appendix B to the proposed order identifies Defendants' specific harmful IP addresses and identifies the specific data centers and hosting companies in two locations through which Defendants registered the IP addresses. The hosting companies are directed to redirect Defendants' Harmful IP Addresses to secure computers, in order to preserve evidence available through them and thereafter disable them prevent the abuse currently carried out through the IP addresses.

Regarding the computers and related materials to be seized at the hosting companies, the proposed order directs the U.S. Marshals Service to carry out service of the order and direct redirection of the IP addresses and seizure of the computers, servers, electronic data storage devices, software, data or media that correspond to the Harmful IP Addresses assigned to Defendants. This material is readily ascertainable because each IP address corresponds to computers in the hosting companies' possession, custody or control. The proposed order directs the hosting companies to redirect the IP addresses to secure computers and isolate and turn over to the U.S. Marshals Service the botnet software and related content on the computers associated with these domains and IP addresses.

The proposed order also identifies categories of records and documents to be seized or provided, including information relating to the identity of Defendants using the Harmful IP Addresses and all logs associated with these servers, all of which is readily ascertainable. This information will enable Microsoft to effect notice and service of process on Defendants.

These categories are sufficiently specific to allow the U.S. Marshals Service, the hosting company and third-party forensic experts under contract with Microsoft to locate the material to be seized without undue burden. As Microsoft anticipates that some of the material to be seized will be electronic data files, it requests the Court to issue a writ of assistance allowing forensic experts to assist with identification of electronic data and media that contain the malicious code. A district court has the power to issue a writ of assistance that compels third parties with technical skills to assist in the technical implementation of a court's order. *See Dell, Inc.*, 2007 U.S. Dist. LEXIS 98676 at *12-13 (citing *United States v. New York Tel. Co.*, 434 U.S. 159, 176 (1977)). The third-party experts will hold the material in secure escrow as the case proceeds.

6. The Harm To Microsoft And The Public Of Denying The Requested Relief Outweighs The Harm To Any Legitimate Interests Of Defendants

As previously established, if the requested relief is denied, serious and irreparable harm to Microsoft, its customers and the public will result. By contrast, Defendants will suffer no harm to any legitimate interest if an *ex parte* TRO and seizure Order issues, as the malicious Citadel Botnets' command and control code operating from the servers at those Harmful Domains and IP Addresses is used solely to propagate and control the Citadel Botnets and not for any legitimate or lawful purpose. Further, as discussed, the impact of the requested relief to the third party domain registries and hosting companies will be negligible, as the order disables access to only a handful of their customers engaged in illegal conduct and seeks these companies' reasonable assistance in the isolation and seizure of the botnet code.

Because each unique Harmful Domain or IP Address is associated with a specific command and control server, identifying and isolating the malicious code onto secure computers and disabling that code should result in only minimal burden to the domain registries and hosting companies. The actions requested are well within the ordinary course of these companies' activities generally and their abuse response activities specifically. Microsoft moreover, will utilize forensic experts to expedite the seizure and further minimize any potential burden.

The Harmful Domains are all solely used by Defendants to carry out the botnet and investigation has revealed only botnet-related activity related to the Harmful IP Addresses. If any third party were found to host content on any of the IP Addresses listed, the impact would be negligible. Such content can be quickly and readily moved by the relevant hosting provider to another IP address and the owners/operators of the content can be promptly notified of the change in IP address. Microsoft and its counsel have carried out such orders successfully in the past, using the same methods sought here.

7. Defendants Are Likely To Destroy, Move, Hide Or Conceal Evidence If Provided Notice

As discussed in detail, Defendants are likely to remove the malicious code and relocate it to new servers if they are provided notice. As such, an *ex parte* TRO and seizure order redirecting the Domains and IP Addresses to secure computers and directing seizure of Defendants' command and control servers is necessary.

8. The All Writs Act Authorizes The Court To Direct Third Parties To Perform Acts Necessary To Avoid Frustration Of The Requested Relief

Microsoft's Proposed Order directs that the third-party domain registries and IP address hosting companies, through which Defendants procured the Harmful Domains and IP Addresses, reasonably cooperate to effectuate the order. Critically, these third-parties are the *only* entities that can effectively disable Defendants' domains and IP addresses and preserve the evidence, and thus their cooperation is necessary.

The All Writs Act provides that a court may issue all writs necessary or appropriate for the administration of justice. 28 U.S.C. § 1651(a). The Supreme Court has recognized that narrow direction to third-parties necessary to effect the implementation of a court order is authorized by the All Writs Act:

> The power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing,

> are in a position to frustrate the implementation of a court order or the proper administration of justice, and encompasses even those who have not taken any affirmative action to hinder justice.

United States v. New York Tel. Co., 434 U.S. at 174 (citations omitted) (order to telephone company to assist in implementation of a pen register warrant was authorized under the All Writs Act); *see also In re Application of United States for an Order Authorizing An In-Progress Trace of Wire*, 616 F.2d 1122, 1129 (9th Cir. 1980) (same; noting of *New York Tel. Co.*, "the Court made the commonsense observation that, without the participation of the telephone company, 'there is no conceivable way in which the surveillance authorized could have been successfully accomplished.'"); *Dell Inc. v. BelgiumDomains, LLC*, 2007 U.S. Dist. LEXIS 98676 (S.D. Fla. Nov. 20, 2007) (All Writs Act applied in conjunction with trademark seizure under Rule 65 and Lanham Act).

Requiring these third parties to reasonably assist in the execution of this order will not offend due process as the Proposed Order requires (1) only minimal assistance from the third parties in executing the order (acts that they would take in the ordinary course of their operations), (2) that it be implemented with the least degree of interference with the normal operation of third parties, (3) does not deprive the third parties of any tangible or significant property interests and (4) requires Microsoft to compensate the third-parties for the assistance rendered. If, in the implementation of the Proposed Order, any third-party wishes to bring an issue to the attention of the Court, Microsoft will bring it immediately. The third-parties, moreover, will have an opportunity to be heard at the preliminary injunction hearing, which must occur shortly after the execution of the Proposed Order, and thereafter. Fed. R. Civ. P. 65(b)(2). The directions to third-parties in the Proposed Order are thus narrow, satisfy Due Process, and are necessary to effect the requested relief.

C. Microsoft Will Make Extraordinary Efforts To Provide Notice Of The TRO And The Preliminary Injunction Hearing And To Serve The Complaint

To ensure Due Process, immediately upon entry of the requested *ex parte* TRO, Microsoft will undertake extraordinary efforts to provide formal and informal notice of the preliminary injunction hearing to Defendants and to serve the complaint. In order to carry out service, the proposed TRO also directs the relevant hosting companies and domain registrars/registries to provide all contact information for the Defendants through which notice may be provided.

Courts in the Fourth Circuit permit discovery to determine the identity of unknown defendants. *Njoku v. Unknown Special Unit Staff*, 217 F.3d 840, 2000 U.S. App. LEXIS 15695, at * 2 (4th Cir. July 7, 2000) (per curiam) (unpublished table decision) (holding that John Doe suits are permitted when "the identity of the alleged defendant is not known at the time the complaint is filed and the plaintiff is likely to be able to identify the defendant after further discovery"). Expedited discovery is permitted in preparation of a preliminary injunction hearing. *See K.G. Holding Corp. v. Union Bank*, 56 Fed. Appx. 111, 114 (4th Cir. 2003) ("The parties engaged in expedited discovery in preparation for the ... hearings ... for preliminary injunction."); *CIENA Corp. v. Jarrard*, 203 F.3d 312, 315 (4th Cir. 2000) (remanding to give the defendant an opportunity to conduct expedited discovery before the district court's reconsideration of preliminary injunction motion). For expedited discovery to prepare for preliminary injunction hearings, courts in the Fourth Circuit have adopted a "reasonableness" or "good cause" standard, taking into account the totality of the circumstances. *See Dimension Data N. Am., Inc. v. NetStar-1, Inc.*, 226 F.R.D. 528, 531 (E.D.N.C. 2005) (finding that the four-factor test from in *Notaro v. Koch*, 95 F.R.D. 403, 405 (S.D.N.Y. 1982), is not appropriate for expedited discovery to prepare for preliminary injunction hearings and adopting a "reasonableness" or "good cause" standard instead).

The discovery requested here is reasonable as it is necessary to identify Defendants in order to serve them and hold them accountable for their unlawful conduct. Defendants are real people who have created and now direct the daily operation of the Citadel Botnets. If identified, they will be amenable to suit in federal court. Microsoft has diligently researched the Citadel Botnets, and has identified the Harmful Domains and IP Addresses that comprise the Command and Control Tier of the botnet set up by Defendants. Microsoft's investigation into Defendants' identities can progress no further until it gains access to more information related to the specific identities of the Defendants, as Defendants routinely use fake registration information in public WHOIS records. The requested information is necessary to identify the Defendants, serve them with process, and prosecute this case. At this point in the proceedings, Microsoft's requests for contact information will be made only to service providers providing support for the critical botnet infrastructure. Accordingly, good and compelling cause exists to grant Microsoft's narrow request for Doe discovery.

Microsoft Will Provide Notice By E-mail, Facsimile, Mail: Microsoft will provide notice of the preliminary injunction hearing and will effect service of the Complaint by immediately sending all pleadings to the e-mail and messaging addresses, facsimile numbers and mailing addresses associated with Defendants or provided by Defendants to domain registrars/registries and hosting companies in relation to the command and control infrastructure. When Defendants registered for domain names and hosting services, they agreed not to engage in abuse such as that at issue in this case and agreed that notice of disputes regarding domain or IP address hosting could be provided to them by sending complaints to the e-mail, facsimile and mail addresses provide by them. *See* Cox Decl. ¶¶28-31, Ex. 7.

Microsoft Will Provide Notice To Defendants By Publication: Microsoft will notify the Defendants of the preliminary injunction hearing and the complaint against their misconduct by publishing the materials on a centrally located, publically accessible source on the Internet for a period of 6 months. Microsoft will also affect notice by additional publication methods as may be directed by the Court as the case proceeds.

Microsoft Will Provide Notice By Personal Delivery And Treaty If Possible: If valid physical addresses of Defendants can be identified, Microsoft will notify Defendants and serve process upon them by personal delivery or through the Hague Convention on service of process or similar treaty-based means.

Notice and service by the foregoing means satisfy Due Process, are appropriate, sufficient and reasonable to apprise Defendants of this action and are necessary under the circumstances. Microsoft hereby formally requests that the Court approve and order the alternative means of service discussed above. The Court can order Microsoft's proposed methods of notice and service under Federal Rule of Civil Procedure 4(f)(3) which authorizes service by "other means" that are "not prohibited by international agreement." *BP Prods. N. Am. Inc. v. Dagra*, 232 F.R.D. 263, 264 (E.D. Va. 2005). A party need not have attempted every permissible means of service before petitioning the court for alternative relief under Rule 4(f)(3) as it stands on equal footing with other methods of service Rule 4 authorizes. *See id.* ("Service of process under Rule 4(f)(3) is neither a 'last resort' nor 'extraordinary relief.'") (quoting *Rio Props., Inc. v. Rio Int'l Interlink*, 284 F.3d 1007, 1015 (9th Cir. 2002)).

In this case, the e-mail addresses provided by Defendants to the domain registrars / registries and hosting companies, in the course of obtaining services that support the botnet, are likely to be the most accurate and viable contact information and means of notice and service.

Cox Decl. ¶6. Defendants, moreover, will expect notice regarding their use of these services to operate their botnet by those means, as Defendants agreed to such in their domain registration and hosting agreements. *See Nat'l Equip. Rental, Ltd. v. Szukhent,* 375 U.S. 311 (1964) ("And it is settled. . . that parties to a contract may agree in advance to submit to the jurisdiction of a given court, to permit notice to be served by the opposing party, or even to waive notice altogether."). For these reasons, notice and service by e-mail and publication are warranted and necessary here.[6]

Microsoft's proposed methods of notice and service by e-mail, facsimile, mail and publication also satisfy Due Process as these means are reasonably calculated, in light of the circumstances, to apprise the interested parties of the TRO, the preliminary injunction hearing and the lawsuit. *See Mullane v. Cent. Hanover Bank & Trust Co.*, 339 U.S. 306, 314 (1950). *See, e.g., Smith v. Islamic Emirate of Afghanistan*, 2001 U.S. Dist. LEXIS 21712, *8-11 (S.D.N.Y. 2001) (authorizing service by publication upon Osama bin Laden and the al-Qaeda organization); *Rio Prop., Inc.,* 284 F.3d at 1014-15 (authorizing service by e-mail upon an international defendant); *FMAC Loan Receivables v. Dagra*, 228 F.R.D. 531, 535-36 (E.D. Va. 2005) (acknowledging that courts have readily used Rule 4(f)(3) to authorize international service through non-traditional means); *BP Prods. N. Am., Inc. v. Dagra,* 236 F.R.D. 270, 271-73 (E.D. Va. 2006) (approving notice by publication); *AllscriptsMisys, LLC*, 2010 U.S. Dist. LEXIS 4450, at *3 (granting *ex parte* TRO and order prompting "notice of this Order and Temporary Restraining Order as can be effected by telephone, electronic means, mail or

[6] Additionally, if the physical addressees provided by Defendants to hosting companies turns out to be false and Defendants' whereabouts are unknown, the Hague Convention will not apply in any event and alternative means of service, such as email and publication, would be appropriate for that reason as well. *See BP Prods. N. Am., Inc.*, 236 F.R.D. at 271 ("The Hague Convention does not apply in cases where the address of the foreign party to be served is unknown.")

delivery services."); *Microsoft Corp. v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va. 2010, Brinkema J.) at Dkt. 38, pg 4 (authorizing notice of preliminary injunction and service on botnet operators by e-mail, facsimile, mail and publication).

Such service is particularly warranted in cases such as this involving Internet-based misconduct, carried out by international defendants, causing immediate, irreparable harm. As the Ninth Circuit recently observed:

> [Defendant] had neither an office nor a door; it had only a computer terminal. If any method of communication is reasonably calculated to provide [Defendant] with notice, surely it is e-mail-the method of communication which [Defendant] utilizes and prefers. In addition, e-mail was the only court-ordered method of service aimed directly and instantly at [Defendant]. . . Indeed, when faced with an international e-business scofflaw, playing hide-and-seek with the federal court, e-mail may be the only means of effecting service of process.

Rio Props., Inc., 284 F.3d at 1014-1015;[7] *see also Williams-Sonoma, Inc. v. Friendfinder, Inc.*, 2007 U.S. Dist. LEXIS 31299, *5-6 (N.D. Cal. 2007) (service by e-mail consistent with Hague Convention and warranted in case involving misuse of Internet technology by international defendants).

For all of the foregoing reasons, Microsoft respectfully request that the Court enter the requested TRO, seizure order and order to show cause why a preliminary injunction should not issue, and further order that the means of notice of the preliminary injunction hearing and service of the complaint set forth herein meet Fed. R. Civ. Pro. 4(f)(3), satisfy Due Process and are reasonably calculated to notify Defendants of this action.

[7] *Rio Properties* has been followed in the Fourth Circuit. *See FMAC Loan Receivables*, 228 F.R.D. at 534 (E.D. Va. 2005) (following *Rio*); *BP Prods. N. Am, Inc.*, 232 F.R.D. at 264 (E.D. Va. 2005) (same); *Williams v. Adver. Sex L.L.C.*, 231 F.R.D. 483, 486 (N.D. W. Va. 2005) ("The Fourth Circuit Court of Appeals has not addressed this issue. Therefore, in the absence of any controlling authority in this circuit, the Court adopts the reasoning of the Ninth Circuit in *Rio Properties, Inc.* ...)

III. CONCLUSION

For the reasons set forth herein, Microsoft respectfully requests that this Honorable Court grant its motion for a TRO, seizure order and order to show cause regarding a preliminary injunction. Microsoft further respectfully requests that the Court permit notice of the preliminary injunction hearing and service of the Complaint by alternative means.

Dated: May 29, 2013

By: ______________________________
Neil T. Bloomfield
NC Bar No. 37800

Moore & Van Allen PLLC
100 North Tryon Street
Suite 4700
Charlotte, NC 28202-4003
Telephone: +1-704-331-1084
Facsimile: +1-704-409-5660
Email: neilbloomfield@mvalaw.com

Of counsel:

Gabriel M. Ramsey
(*pro hac vice* application pending)
Attorney for Plaintiff Microsoft Corp.

Orrick, Herrington & Sutcliffe LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401
Email: gramsey@orrick.com

Jeffrey L. Cox
(*pro hac vice* application pending)
Attorney for Plaintiff Microsoft Corp.

Orrick, Herrington & Sutcliffe LLP
701 5th Avenue, Suite 5600
Seattle, WA 98104-7097
Telephone: (206) 839-4300
Facsimile: (206) 839-4301
Email: jcox@orrick.com

James M. Hsiao
(*pro hac vice* application pending)
Attorney for Plaintiff Microsoft Corp.

Orrick, Herrington & Sutcliffe LLP
777 South Figueroa Street
Suite 3200
Los Angeles, CA 90017-5855
Telephone: (213) 612-2449
Facsimile: (213) 612-2499
Email: jhsiao@orrick.com

Attorneys for Plaintiff