

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. _____

COMPLAINT

Plaintiffs MICROSOFT CORP. ("Microsoft"), hereby complains and alleges that JOHN DOES 1-82 ("John Does" or "Doe Defendants") are controlling a worldwide series of interconnected illegal computer networks, collectively known as the "Citadel Botnets," comprised of end-user computers connected to the Internet that Defendants have infected with malicious software. Defendants have used the Citadel Botnets to infect millions of computers on the Internet, which were then used to steal millions of dollars during the past year and a half. Defendants control the Citadel Botnets through a sophisticated command and control infrastructure hosted at and operated through Internet domains set forth at Appendix A (hereinafter the "Harmful Domains") and the Internet Protocol addresses set forth at Appendix B to this Complaint (hereinafter the "Harmful IP Addresses") (herein collectively referred to as the "Harmful Domains and IP Addresses"), as follows:

NATURE OF ACTION

1. This is an action based upon: the Computer Fraud and Abuse Act (18 U.S.C. § 1030); CAN-SPAM Act (15 U.S.C. § 7704); Electronic Communications Privacy Act (18 U.S.C. § 2701); trademark infringement under the Lanham Act (15 U.S.C. § 1114), false designation of origin under the Lanham Act (15 U.S.C. § 1125(a)); trademark dilution under the Lanham Act (15 U.S.C. § 1125(c)); the Racketeer Influence and Corrupt Organizations Act (18 U.S.C. § 1962(c)); unjust enrichment; computer trespass; common law conversion and nuisance. Microsoft seeks injunctive and other equitable relief and damages against Defendants for their creation, control, maintenance, and ongoing use of the Citadel Botnets, which have caused and continue to cause irreparable injury to Microsoft, Microsoft's customers and the general public.

THE PARTIES

2. Plaintiff Microsoft Corp. is a corporation duly organized and existing under the laws of the State of Washington, having its headquarters and principal place of business in Redmond, Washington. Microsoft is a leading provider of technology products and services, including computer software, Internet services, websites and email services.

3. Microsoft is informed and believes and thereupon alleges that John Doe 1 is the creator of or member of the group that created and provides support and further development to the "Citadel" botnet code that comprise the Citadel Botnets. John Doe 1 goes by the alias "Aquabox" and may be contacted at messaging addresses aquabox@jabber.jp, aquabox@jabber.org, and aquabox@lugmen.org.ar.

4. Microsoft is informed and believes and thereupon alleges that John Does 2 through 82 go by the aliases set forth at Appendix C. Upon information and belief, John Does 2 through 82 operate the Citadel Botnets and can likely be contacted and may be contacted at the

contact information set forth at Appendix C.

5. Microsoft is informed and believes and thereupon allege that John Doe 1, as creator, maintainer and developer of the malicious botnet code, has acted in concert with John Does 2 through 82 who have purchased, developed and/or supported such botnet code, and are currently operating or have contributed to the operation of the Citadel Botnets.

6. Defendants own, operate, control, and maintain the Citadel Botnets through a command and control infrastructure hosted at and/or operating at the Harmful Domains and IP Addresses. The command and control infrastructure hosted and operated at the Harmful Domains and IP Addresses are maintained by the third-party domain registries and hosting companies set forth at Appendices A and B to this Complaint.

7. Plaintiffs are unaware of the true names and capacities of Defendants sued herein as John Does 1-82 inclusive and therefore sue these Defendants by such fictitious names. Microsoft will amend this complaint to allege Defendants' true names and capacities when ascertained. Microsoft will exercise due diligence to determine Defendants' true names, capacities, and contact information, and to effect service upon those Defendants.

8. Microsoft is informed and believes and therefore alleges that each of the fictitiously named Defendants is responsible in some manner for the occurrences herein alleged, and that Microsoft's injuries and the injuries to Microsoft's customers herein alleged are proximately caused by such Defendants.

9. The actions and omissions alleged herein to have been undertaken by Defendants were undertaken by each Defendant individually, were actions and omissions that each Defendant authorized, controlled, directed, or had the ability to authorize, control or direct, and/or were actions and omissions each Defendant assisted, participated in, or otherwise

encouraged, and are actions for which each Defendant is liable. Each Defendant aided and abetted the actions of Defendants set forth below, in that each Defendant had knowledge of those actions and omissions, provided assistance and benefited from those actions and omissions, in whole or in part. Each Defendant was the agent of each of the remaining Defendants, and in doing the things hereinafter alleged, was acting within the course and scope of such agency and with the permission and consent of other Defendants.

JURISDICTION AND VENUE

10. This action arises out of Defendants' violation of the Federal Computer Fraud and Abuse Act (18 U.S.C. § 1030), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125(a), (c)), and the Racketeer Influence and Corrupt Organizations Act (18 U.S.C. § 1962(c)). Therefore, the Court has subject matter jurisdiction over this action based on 28 U.S.C. § 1331. This is also an action for computer trespass, unjust enrichment, conversion and nuisance. This Court, accordingly, has subject matter jurisdiction under 28 U.S.C. § 1367.

11. Defendants have directed acts complained of herein toward the state of North Carolina and the Western District of North Carolina, have utilized instrumentalities located in North Carolina and the Western District of North Carolina to carry out the acts alleged in this Complaint, and engaged in other conduct availing themselves of the privilege of conducting business in North Carolina and the Western District of North Carolina.

12. In particular, Defendants control a network of compromised user computers called the "Citadel Botnets" that Defendants use to conduct illegal activities, thereby causing harm to Microsoft as well as Microsoft's customers and the general public in the Western District of North Carolina. Defendants have directed actions at the Western District of North

Carolina, by directing malicious computer code at computers of individual Internet users located in the Western District of North Carolina, infecting those user computers with the malicious code and thereby making the user computers part of the Citadel Botnets. Figure 1 depicts the geographical location of infected user computers in the Western District of North Carolina.

Figure 1 – Citadel Botnet Computers In The Western District Of North Carolina



13. Defendants have undertaken the foregoing acts with knowledge that such acts would cause harm through user computers located in North Carolina, thereby injuring Microsoft, its customers and others in North Carolina and elsewhere in the United States. Therefore, this Court has personal jurisdiction over Defendants.

14. Pursuant to 28 U.S.C. § 1391(b), venue is proper in this judicial district. A substantial part of the events or omissions giving rise to Microsoft's claims, together with a substantial part of the property that is the subject of Microsoft's claims, are situated in this judicial district. Venue is proper in this judicial district under 28 U.S.C. § 1391(c) because Defendants are subject to personal jurisdiction in this judicial district.

15. Plaintiff Microsoft has been directly injured through the activities alleged herein

and brings this action on its own behalf.

FACTUAL BACKGROUND

Microsoft's Products, Services And Reputation

16. Plaintiff Microsoft® is a provider of the Windows® operating system, the Internet Explorer® browser and the Outlook®, Hotmail®, Windows Live® and MSN® email and messaging services and a variety of other software and services. Microsoft has invested substantial resources in developing high-quality products and services. Due to the high quality and effectiveness of Microsoft's products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, establishing a strong brand and developing the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. Microsoft has registered trademarks representing the quality of its products and services and its brand, including the Microsoft®, Windows®, Internet Explorer® and other marks. True and correct copies of Microsoft's trademark registrations are attached as Appendix D.

17. Defendants, by operating, controlling, maintaining, and propagating the Citadel Botnets have caused and continue to cause severe and irreparable harm to each Plaintiff, their customers, their members, and the public at large.

Computer "Botnets"

18. In general, a "botnet" is a collection of individual computers running software that allows communication among those computers and that allows centralized or decentralized communication with other computers providing control instructions. A botnet network may be comprised of multiple, sometimes millions, of end-user computers infected with the malicious

software (“malware” or “Trojan”). The individual computers in a botnet often belong to individual end-users who have unknowingly downloaded or been infected by such software that makes the computer part of the botnet. An end-user’s computer may become part of a botnet when the user inadvertently interacts with a malicious website advertisement, clicks on a malicious email attachment, or downloads malicious software. In each such instance, software code is downloaded or executed on the user’s computer, causing that computer to become part of the botnet, capable of sending and receiving communications, code, and instructions to or from other botnet computers.

19. Criminal organizations and individual cyber criminals often create, control, maintain, and propagate botnets in order to carry out misconduct that harms others’ rights. They use botnets because of botnets’ ability to support a wide range of illegal conduct, their resilience against attempts to disable them, and their ability to conceal the identities of the malefactors controlling them. The controllers of a botnet will use an infected end-user computer for a variety of illicit purposes, unknown to the end user. A computer in a botnet, for example, may be used to:

- a. carry out theft of credentials and information, fraud, computer intrusions, or other misconduct;
- b. anonymously send unsolicited bulk email without the knowledge or consent of the individual user who owns the compromised computer;
- c. deliver further malicious software that infects other computers, making them part of the botnet as well; or
- d. “proxy” or relay Internet communications originating from other computers, in order to obscure and conceal the true source of those communications.

Botnets provide a very efficient general means of controlling a huge number of computers and targeting any action internally against the contents of those computers or externally against any computer on the Internet.

20. Microsoft brings this action to stop Defendants from controlling, maintaining, and growing the Citadel Botnets that have caused harm to Microsoft, its customers and to the general public. Defendants control, maintain, and grow the Citadel Botnets through the command and control infrastructure hosted at and operated through the Harmful Domains and IP Addresses described herein and set forth at Appendices A and B.

The “Citadel Botnets”

21. The Citadel Botnets primarily carry out theft of account credentials for websites, particularly online banking websites. The Citadel Botnets’ primary aim is to infect end-user computers in order to (1) steal the users’ online account credentials, including online banking credentials, (2) access consumers’ accounts with the stolen credentials, and (3) steal information from consumers’ website accounts and steal funds from consumers’ banking and financial accounts. The creators of the Citadel Botnets’ malicious code, moreover, collaborate in a common operation to create, distribute, and operate the Citadel Botnets. The resulting harm to Microsoft, its end-user customers, financial institutions, government agencies and the general public is the result of a single global criminal operation that controls, operates, and maintains the Citadel Botnets.

Defendants Work Together In A Common Operation To Create, Control, And Maintain The Citadel Botnets

22. The Citadel Botnets comprise a family of inter-related botnets – known on the Internet as the “Citadel” botnets. The “Citadel” botnets are built on similar software code and infrastructure as their progenitor, the “Zeus” botnet. Defendant John Doe 1, the creator and

developer of the Citadel botnet code – whose specific identity is currently unknown – has operated in anonymity on the Internet for several years. John Doe 1 has offered the Citadel botnet code for sale on the Internet as “builder kits” that allow others, including the other Defendants, to easily setup, operate, maintain, and propagate botnets to infect end-user computers, carry out financial theft, send spam email or engage in other malicious activities. Depending on the level of sophistication in particular versions, and the level of support and customization provided, the code may cost from approximately \$2,400 or more for comprehensive or tailored versions. These kits contain software that enable other Defendants to generate executable botnet code, configuration files, and web server files that they deploy on command and control servers.

23. The “Citadel” botnet code first emerged in approximately January 2012. The “Citadel” code evolved over time, becoming more sophisticated and including additional features designed to counter attempts to analyze and disable the botnet.

24. John Doe 1 provides a high degree of after-sales service to the other Defendants. 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. Using Citadel CRM, the other Defendants can report problems, propose and suggest and vote on new features, and exchange ideas and best practices with other Citadel botnet operators. 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. John Does 1-82 actively collaborate, day-to-day,

on the development and operation of Citadel.

25. For example, using the Citadel CRM, John Doe 1 proposed a new feature on January 13, 2012 and solicited the feedback of John Does 2-82. The proposed feature is giving Citadel bots their own antivirus capability that would allow them to clean other competing malware infections and “adware” off the end-user’s computer. By doing so, 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. 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. The Figure below shows a screen shot of the Citadel CRM displaying the foregoing communications:

Mini-antivirus in the Citadel

support

January 13, 2012

And you interesting mini-antivirus in our software that will clean up a variety of Malware 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 \favclean\ in the configuration, software decision: to pump. All from the server, with integrated antivirus 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 the anti-virus engine will be built based on ClamAV. Key signatures ClamAV weigh about 2 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:
do not do:

The final decision: in

Need I possess. Your price: _____

☐ Useful, but I do not need

☐ Absolutely not needed

☐ No need, I do not possess

Vote

Comments to the module

bigalk

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

Dares

a minimum of 2448 and 80960 killer)

26. John Doe 1 has been swift to add new features and fix bugs and has released multiple versions on a fast schedule to provide the Citadel botnet operators with the latest updates. The fast pace of updates demonstrates the intensity and the amount of work being done to make Citadel a robust instrument for cybercrime and the level of cooperation between the Citadel developers and their customers. In the first six months that Citadel was available, John Doe 1 released five versions of the build-kit.

27. John Doe 1 is the developer of Citadel. He has developed and commercialized Citadel by (1) designing and developing the Citadel bot code and all of the modules that enable a Citadel bot to conduct theft; (2) creating a build-kit that customers can purchase and then use to quickly generate bots and configuration files, which are the primary means of conducting financial theft; (3) selling the Citadel build-kits 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 (4) offering to collaborate and work-for-hire to add new features.

Defendants Work Together To Operate The Citadel Botnets

28. Microsoft is informed and believes and thereupon alleges that the common code and characteristics of the Citadel botnets, and evidence regarding specific activities of the Defendants, demonstrate that the Citadel Botnets are controlled by a number of Defendants acting in concert. Upon information and belief, John Doe 1, the creator and provider of the botnet code, works together with the purchasers, developers and other sellers of the Citadel Botnet code in a continuous and coordinated manner to control, operate, distribute, and maintain the Citadel Botnets. Upon information and belief, the malicious software that Defendants install on end-user machines all share common code and characteristics, and have evolved over time to

more closely resemble one another.

29. John Does 2-82 have purchased the Citadel Botnet code and, in concert with the creator of the code, are deploying and operating the Citadel Botnets. Each of John Does 2-82 has participated in the Citadel enterprise through the following acts: (1) Purchasing a Citadel build kit and using it to generate bots and configuration files to control the bots; (2) Deploying the bots under one or more botnet names; (3) Creating a command and control infrastructure made of server computers connected to the Internet through which to communicate with the deployed bots; (4) Using one or more means to cause end-user computers to become infected with Citadel; (5) Using the Citadel bots infecting the computers of end-users around the world to steal security identification and financial account information; (6) Using Citadel bots to steal money directly from the financial accounts of unsuspecting end-users around the world; (7) Damaging Microsoft-owned and licensed software including Windows and Internet Explorer, corrupting the behavior of these programs to convert them to instruments of criminality; (8) 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; (9) Using Citadel bots to send illegal spam e-mail; (10) Using Citadel bots to cause secondary infections, such as by the "Reveton" ransomware, which demands payment to unlock the victim computer; and (11) Using Citadel bots to launch distributed denial of service attacks on financial and other institutions.

30. John Doe 1, the Defendant creator of the botnet code works together with these Defendant operators of the botnets in a continuous and coordinated manner to control, operate, distribute, and maintain the Citadel Botnets. John Doe 1 continually provides updates and instruction to John Does 2-82 regarding deployment and operation of the Citadel Botnets.

The Citadel Racketeering Enterprise

31. 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.

32. Upon information and belief, John Does 1-82 constitute a group of persons associated together for a common purpose of engaging in a course of conduct, as part of an ongoing organization, with the various associates functioning as a continuing unit. The Defendants' enterprise has a purpose, with relationships among those associated with the enterprise, and longevity sufficient to permit those associates to pursue the enterprise's purpose. Upon information and belief, Defendant John Does 1 through 82 conspired to, and did, form an associated in fact enterprise (herein after the "Citadel Racketeering Enterprise") with a common purpose of developing and operating a global credential stealing botnet operation as set forth in detail herein.

33. The Citadel Racketeering Enterprise has existed since at least January of 2012, when John Doe 1 presented the single, consolidated global credential stealing botnet in public. Other Defendants identified as John Does 2-82 joined and began participating in the Citadel Enterprise at various times thereafter.

34. The Citadel Racketeering Enterprise has continuously and effectively carried out its purpose of developing and operating a global credential stealing botnet operation since that time, and will continue to do so absent the judicial relief that Microsoft requests.

35. Both the purpose of the Citadel Racketeering Enterprise and the relationship

between the Defendants is proven by: (1) the emergence of the Citadel botnet; (2) the subsequent development and operation of the Citadel botnet; and (3) Defendants' respective and interrelated roles in the sale, operation of, and profiting from the Citadel Botnets in furtherance of Defendants' common financial interests.

36. Upon information and belief, Defendants have conspired to, and have, conducted and participated in the operations of the Citadel Racketeering Enterprise through a continuous pattern of racketeering activity as set forth herein. Each predicate act is related to and in furtherance of the common unlawful purpose shared by the members of the Citadel Racketeering Enterprise. These acts are continuing and will continue unless and until this Court grants Microsoft's request for a temporary restraining order.

37. Upon information and belief, Defendants have conspired to, and have, knowingly and with intent to defraud used a counterfeit access device in the form of a Windows XP product key to install and activate an unauthorized copy of Windows XP in order to produce the necessary Citadel botnet software operated by Defendants.

38. As set forth in detail herein, Defendants have used the counterfeit access code to install and activate numerous unauthorized copies of Windows XP in order to establish a common programmatic environment so that other Defendants can craft and compile the necessary Citadel botnet software for use in the Citadel botnet, and in furtherance of their common financial goal of obtaining unauthorized access devices as detailed below.

39. Upon information and belief, Defendants have 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 Botnets created and operated by Defendants.

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

41. Upon information and belief, Defendants have also conspired to, and have, knowingly and with intent to defraud, possessed, and do possess, thousands of such unauthorized access devices fraudulently obtained as described herein.

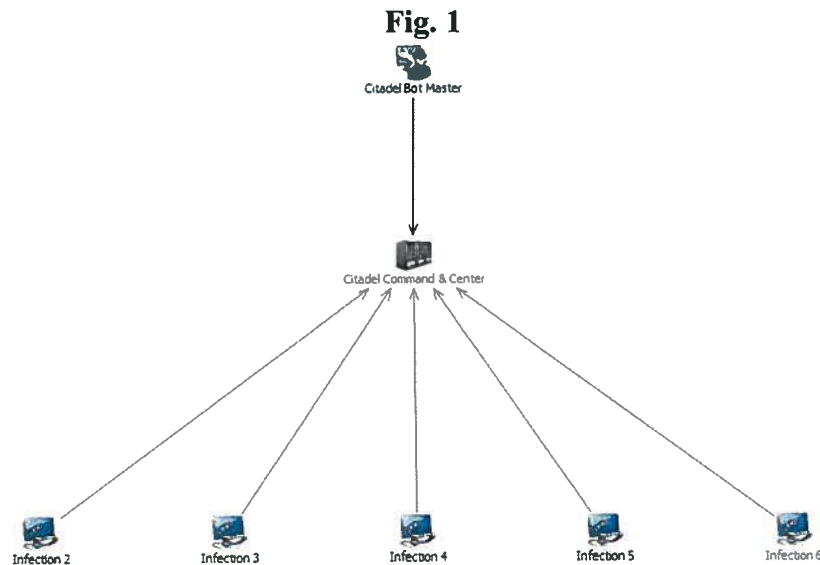
42. Upon information and belief, Defendants have conspired to, and have, knowingly and with intent to defraud, effected transactions with the stolen unauthorized access devices to receive millions of dollars in payment from individuals' bank accounts.

43. Upon information and belief, Defendants have conspired to, and have, executed a scheme to defraud scores of financial institutions by enabling members of the Citadel Racketeering Enterprise to fraudulently represent themselves as specific bank customers, thereby enabling them to access and steal funds from those customer accounts.

44. Each of the foregoing illegal acts were conducted using interstate ACH and/or interstate and/or foreign wires as described herein, and therefore affected interstate and/or foreign commerce.

The Structure Of The Citadel Botnets

45. Citadel botnets have a two-tiered architecture. The lowest tier is referred to as the "Infection Tier," which is made up of bots running on infected end-user computers. The second tier is a "Command and Control Tier" through which the botnet operator communicates with and controls the bots. The tiered architecture of the Citadel botnets can be represented as follows:



1. The Citadel Infection Tier

46. 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. These end-user computers are of the type commonly found in businesses, living rooms, schools, libraries, and Internet cafes around the world. 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.

2. The Citadel Command and Control Tier

47. The second level of the Citadel botnet architecture is referred to as the “Command and Control Tier.” This consists of specialized computers, also connected to the Internet, which run specialized software. 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.

48. 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, approximately every 20 minutes. 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. Servers in the command and control tier include the servers at the domain names and IP addresses at Appendices A and B hereto.

Defendants Use The Harmful Domains And IP Addresses To Infect And Control End-User Computers And To Steal Information And Money From Victims

1. Creation Of Citadel Botnet Code And Configuration File

49. To create a Citadel botnet, Defendant John Does 2 through 82 and others begin by purchasing a Citadel Builder Kit from John Doe 1. 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. 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. In Citadel’s lexicon, the “bot” is the module that will be downloaded onto an end-user’s computer to infect and control it. 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. The Figure below shows a screen shot taken from a Citadel Builder Kit.



50. John Doe 1 urges his customers to build the bot code on computers running Windows XP. 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. In order to provide his botnet customers with access to Windows XP without having to pay Microsoft for it, John Doe 1 provides a stolen version of Windows XP and a stolen product key for Windows XP. The Figure set forth below shows a section taken from the Citadel build kit manual. It gives Citadel customers a path to a version of Windows XP, and provides, in red, a stolen product key for that copy of Window XP.

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. Creation Of Citadel Command And Control Infrastructure

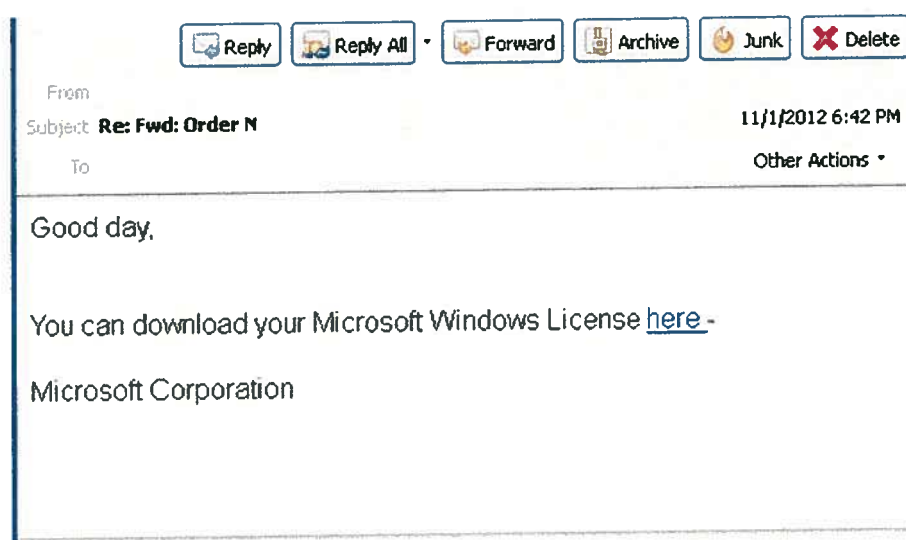
51. In addition to the code and configuration files created using the Citadel Builder Kit, a Citadel botnet operator needs to set up a command and control infrastructure on the Internet. This is done by setting up accounts with web-hosting providers, which are companies that provide facilities where computers can be connected through high-capacity connections to the Internet. 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. 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.

3. Propagation And Control Of Citadel Botnets

52. 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. Typically, the infection of end-user computers involves using software called a "Trojan downloader." The botnet operator will stage the Trojan downloader on a website that the botnet operator has set up or broken into.

53. The Defendants then typically use lures to cause individuals browsing the Internet to visit these servers. 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. 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. The

Figure below is an example of this spam. It can be seen from this that the Citadel botnet operators misuse the trademarks of well known companies and organization such as Microsoft and other parties, such as NACHA, financial institutions and others to fool the recipient into thinking the spam e-mail is from a legitimate source.



54. 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. If a vulnerability is found, the exploit pack will download the Trojan onto the end-user’s computer. This will result in the installation of the Citadel bot on the end-user’s computer. 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. The software and computer are used to carry out malicious activity, described below.

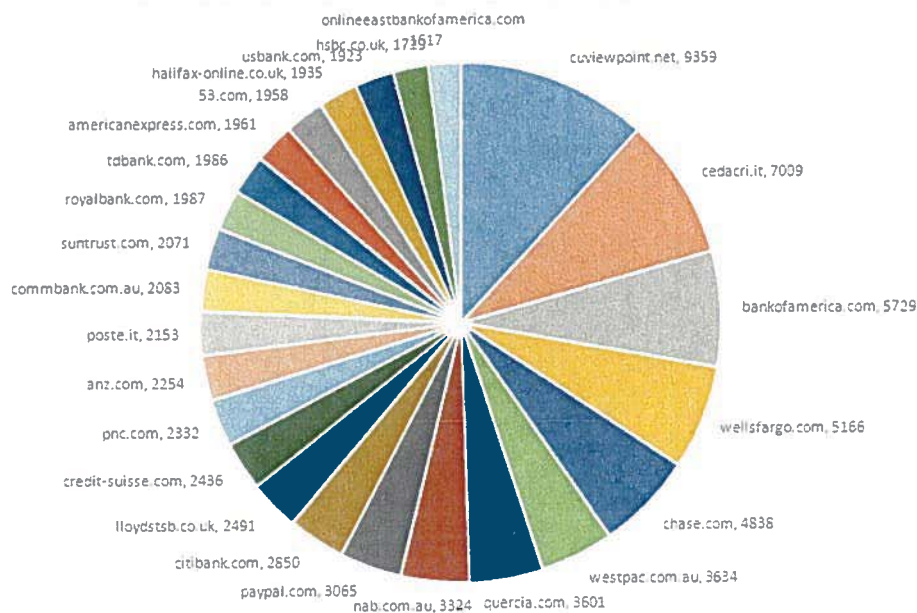
55. After it is installed, a Citadel bot is programmed to contact one to five command and control computers on the Internet. These are referred to as the “base domains,” because they are the first domains that a Citadel bot will attempt to contact, and they are included in the original bot executable generated by the Citadel Builder Kit. By studying many thousands of

Citadel bots, Microsoft has developed a list of these base domains.

56. When a Citadel bot establishes contact with one of these base domains, the bot will download an encrypted configuration file from it. Citadel configuration files contain various types of information which will control the operation of the bot on the end-user's computer. By changing the configuration files, the operators of Citadel can control the operation of the infected end-user computers.

57. Citadel configuration files contain a variety of information used by the bot in the day-to-day work of stealing money. This includes 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. At that point, the bot can begin its attack on the user's accounts using a variety of techniques discussed below.

58. The Figure below shows the number of times each of the top 25 Citadel financial institution targets has been listed in a captured configuration file, from a set of configuration files studied by Microsoft. 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 is headquartered in Charlotte, North Carolina.



59. Second, a Citadel configuration file will contain a list of Citadel Command and Control servers with which it is to communicate. 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. 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.

60. 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. 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 law enforcement action against themselves.

4. Defensive Mechanisms Of Citadel Botnets

61. Relevant to the relief Microsoft seeks, Citadel botnets have certain defensive

mechanisms to better withstand technical counter-measures. 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. 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.

62. 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. If a user attempts to connect to a website from which to download anti-virus software, Citadel will block that. When the Citadel bot detects an attempt to connect to an antivirus website, it will hijack and redirect the user's browser. This keeps any antivirus software of 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.

B. Defendants Use Citadel To Steal Money

63. 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. Once the Citadel bot detects that the user has attempted to connect to a targeted financial website, the bot can proceed in several ways. 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. 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.

64. 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. 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. It does this by "injecting" additional code into the website code that the browser is rendering in a displayable format for the user.

65. 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. Citadel is capable of exploiting various browsers in this manner including Microsoft Internet Explorer, Google Chrome, and Mozilla Firefox. The Figure below shows two screen-shots of what example Citadel "web injects" looks like. 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.

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:

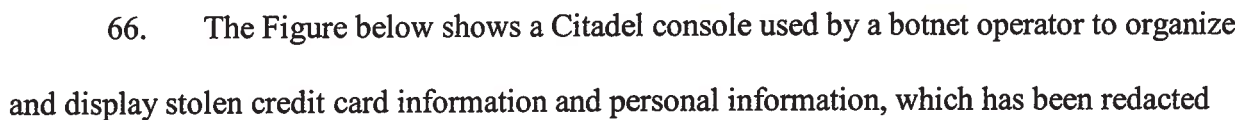
Driver's License Nr:

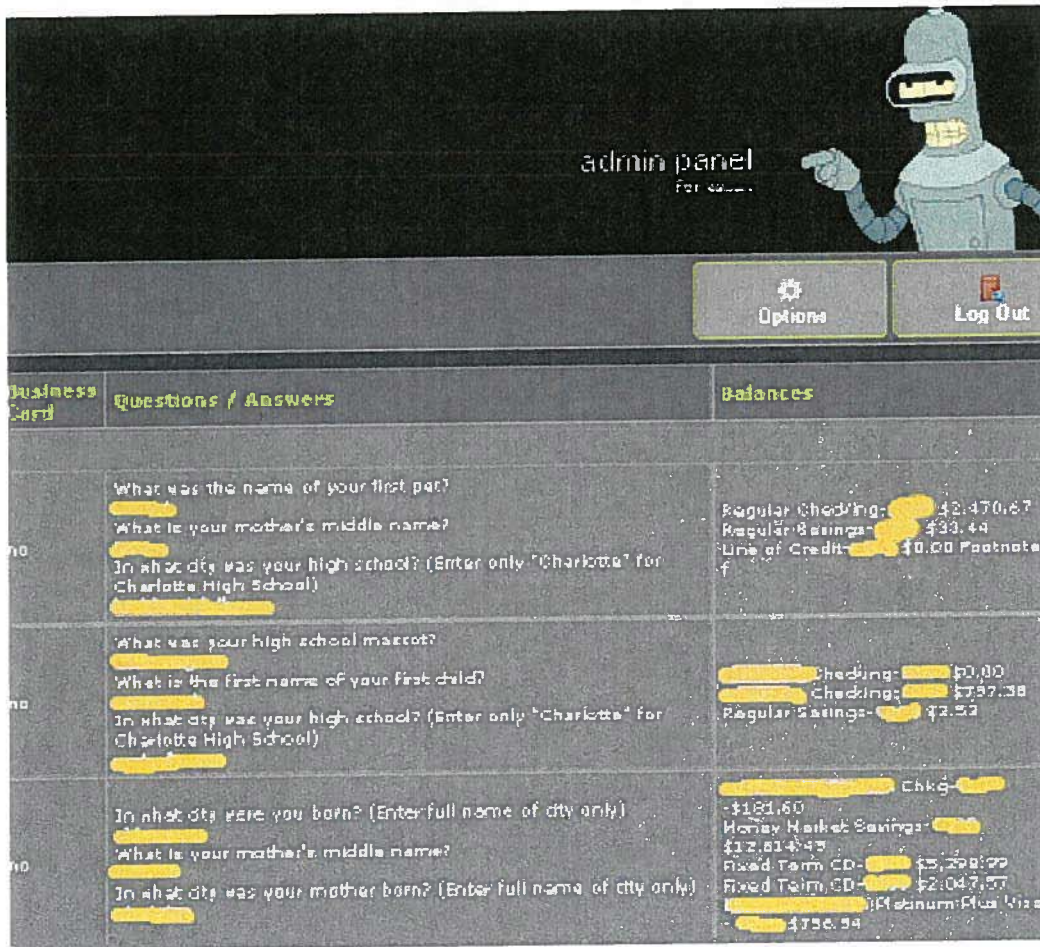
ATM Pin:

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)

continue





67. 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. To do this, it first hijacks the user's browser to keep it from connecting to the real website of the financial institution. 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. The user, believing they are 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. 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. 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. The botnet operators repeatedly misuse the trademarks of financial institutions on these fake online banking websites in order to confuse and mislead victims. This makes it nearly impossible for users to detect the attack.

68. Citadel bots allow the botnet operator to remotely access and operate the infected computer over the Internet. 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. 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. 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.

69. 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.

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

70. 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. 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. 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. 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.

D. Damage To Computers And Microsoft Software

71. 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. 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. 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. Additionally, it makes fundamental changes at the level of the Windows Registry. Microsoft's customers whose computers are infected with the malicious software are damaged by these changes to Windows, which alter the normal and approved settings and functions of the user's operating system, destabilize it, and forcibly draft the customers' computers into the botnet.

72. 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. Yet, they still bear the Microsoft Windows and Internet Explorer trademarks. This is obviously meant to and does mislead Microsoft's customers, and it causes extreme damage to Microsoft's brands and trademarks. Customers are usually unaware of the fact that their computers are infected and have become part of the Citadel botnet. 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. Even with professional assistance, cleaning an infected end-user computer can be exceedingly difficult, time-consuming, and frustrating.

1. Citadel Causes Severe Injury To Microsoft

73. 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. 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. 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.

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

74. 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.

CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF

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

75. Microsoft realleges and incorporates by reference the allegations contained in paragraphs 1 through 74 above.

76. Defendants (1) knowingly and intentionally accessed Microsoft's protected

operating system, software and computers, (2) knowingly and intentionally accessed Microsoft's customers' protected computers, and (3) accessed such protected computers without authorization or in excess of any authorization and knowingly caused the transmission of a program, information, code and commands, and as a result of such conduct intentionally caused damage without authorization to the protected computers (18 U.S.C. § 1030(a)(5)(A)), and; intentionally accessed the protected computers without authorization, and as a result of such conduct caused damage and loss (18 U.S.C. § 1030(a)(5)(C)).

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

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

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

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

SECOND CLAIM FOR RELIEF

Violation of CAN-SPAM Act, 15 U.S.C. § 7704

81. Microsoft realleges and incorporates by reference the allegations contained in paragraphs 1 through 80 above.

82. Microsoft is a provider of Internet access service. Microsoft enables users to access content, including proprietary content, electronic mail, and other Internet services.

83. Defendants initiated the transmission of unsolicited bulk spam e-mail, which are commercial electronic messages, through computers used in interstate and foreign commerce and communication, to thousands or millions of computers, which are also used in interstate and

foreign commerce and communication and are “protected computers” as defined by 18 U.S.C. § 1030(e)(2)(B).

84. By sending messages Defendants initiated the transmission of commercial electronic mail messages to protected computers that contained materially false or misleading header information in violation of 15 U.S.C. § 7704(a)(1).

85. Defendants initiated the transmission of commercial electronic messages to protected computers with actual or fairly implied knowledge that the subject headings of the messages would likely materially mislead recipients regarding the contents or subject matter of the message in violation of 15 U.S.C. § 7704(a)(2).

86. Defendants transmitted to protected computers commercial e-mail messages that did not contain a functioning return electronic mail address or other Internet-based mechanism that recipients could use to contact Defendants and indicate their desire to opt-out of future messages from Defendants, in violation of 15 U.S.C. § 7704(a)(3).

87. Defendants initiated the transmission to protected computers of commercial electronic messages that did not provide: (a) clear and conspicuous identification that the message was an advertisement or solicitation; (b) clear and conspicuous notice of the right to decline to receive future messages; or (c) a valid physical postal address of the sender, in violation of 15 U.S.C. § 7704(a)(5).

88. Defendants’ unsolicited bulk e-mails were sent as part of a systematic pattern and practice that did not conspicuously display a return electronic mail address by which the recipients could submit to the true sender a reply requesting that no further commercial e-mails be sent to the recipient.

89. As a direct result of Defendants’ actions, Microsoft has suffered harm in an

amount to be determined at trial.

90. Microsoft is entitled to the greater of actual damages or statutory damages in accordance with 15 U.S.C. § 7706(g)(1)(B).

91. On information and belief, Defendants' actions were willful and knowing, entitling Microsoft to aggravated damages in accordance with 15 U.S.C. § 7706(g)(3)(C).

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

THIRD CLAIM FOR RELIEF

Violation Of Electronic Communications Privacy Act, 18 U.S.C. § 2701

93. Microsoft realleges and incorporates by reference the allegations contained in paragraphs 1 through 92 above.

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

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

96. Through this unauthorized access, Defendants had access to, obtained and altered, and/or prevented legitimate, authorized access to wire electronic communications, including but not limited to electronic communications while they were in electronic storage in Microsoft's Windows operating system and Internet Explorer software and the computers running such software.

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

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

FOURTH CLAIM FOR RELIEF

Trademark Infringement Under the Lanham Act – 15 U.S.C. § 1114 *et. seq.*

99. Microsoft realleges and incorporates by reference the allegations contained in paragraphs 1 through 98 above.

100. Defendants have used Microsoft's trademarks in interstate commerce.

101. The Citadel Botnets generate and use counterfeit copies of Microsoft's trademarks in fake and unauthorized versions of the Windows operating system, Internet Explorer software and/or fake websites and in spam email, including through the software operating from and through the Command and Control Servers operating at the Harmful Domains and IP Addresses. By doing so, Defendants are likely to cause confusion, mistake, or deception as to the origin, sponsorship, or approval of the fake and unauthorized versions of the Windows operating system, Internet Explorer software, fake websites and spam e-mail and material promoted through the fake websites and spam e-mail.

102. By using Microsoft's financial institution members' trademarks falsely in connection with spam e-mail and fake websites, Defendants have caused, and are likely to cause, confusion, mistake, or deception as to the origin, sponsorship, or approval of the e-mail and fake websites generated and disseminated by the Citadel Botnets. By doing so, Defendants have caused, and are likely to cause, confusion, mistake, or deception as to the origin, sponsorship, or approval of the conduct, actions, products and services carried out by or promoted by Defendants

and the Citadel Botnets.

103. As a result of their wrongful conduct, Defendants are liable to Microsoft for violation of this provision of the Lanham Act.

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

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

106. Defendants' wrongful and unauthorized use of Microsoft's trademarks to promote, market, or sell products and services constitutes trademark infringement pursuant to 15 U.S.C. § 1114 *et seq.*

FIFTH CLAIM FOR RELIEF

False Designation of Origin Under The Lanham Act – 15 U.S.C. § 1125(a)

107. Microsoft realleges and incorporates by reference the allegations contained in paragraphs 1 through 106 above.

108. Microsoft's trademarks are distinctive marks that are associated with Microsoft and exclusively identify its businesses, products, and services.

109. The Defendants, through the Citadel Botnets, make unauthorized use of Microsoft's trademarks. The Citadel Botnets generate and use counterfeit copies of Microsoft's trademarks in fake and unauthorized versions of the Windows operating system, Internet Explorer software and/or fake websites and in spam email, including through the software operating from and through the Command and Control Servers operating at the Harmful Domains and IP Addresses. By doing so, Defendants are likely to cause confusion, mistake, or deception as to the origin, sponsorship, or approval of the fake websites and spam e-mail and

material promoted through the fake websites and spam e-mail.

110. By using Microsoft's trademarks falsely in connection with fake and unauthorized versions of the Windows operating system, Internet Explorer software and/or spam e-mail and fake websites, Defendants are likely to cause confusion, mistake, or deception as to the origin, sponsorship, or approval of the fake and unauthorized versions of the Windows operating system, Internet Explorer software and/or e-mail and fake websites generated and disseminated by the Citadel Botnets. By doing so, Defendants are likely to cause confusion, mistake, or deception as to the origin, sponsorship, or approval of the conduct, actions, products and services carried out by or promoted by Defendants and the Citadel Botnets.

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

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

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

SIXTH CLAIM FOR RELIEF

Trademark Dilution Under The Lanham Act – 15 U.S.C. § 1125(c)

114. Microsoft realleges and incorporates by reference the allegations contained in paragraphs 1 through 113 above.

115. Microsoft's trademarks are distinctive marks that are associated with Microsoft and exclusively identify its businesses, products, and services.

116. The Citadel Botnets makes unauthorized use of Microsoft's trademarks. By doing so, Defendants are likely to cause dilution by blurring and dilution by tarnishment of Microsoft's

trademarks.

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

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

SEVENTH CLAIM FOR RELIEF
Violations of the Racketeer Influenced and
Corrupt Organizations Act (RICO) – 18 U.S.C. § 1962(c)

119. Microsoft realleges and incorporates by reference the allegations contained in paragraphs 1 through 118 above.

120. Beginning during or before January of 2012 and continuing up through the filing of this Complaint, Defendants John Does 1 through 82 were and are associated in fact with the Citadel Racketeering Enterprise and have conducted its affairs through a pattern of racketeering activity, with such conduct and activities affecting interstate and foreign commerce. At various dates after January 2012 and continuing through the filing of this Complaint, Defendants John Does 2 through 82 became associated in fact with the Citadel Racketeering Enterprise and have also conducted and participated in its affairs through a pattern of racketeering activity that affects interstate and foreign commerce. Defendants have engaged in an unlawful pattern of racketeering activity involving thousands of predicate acts of fraud and related activity in connection with access devices, 18 U.S.C. § 1029, wire fraud, 18 U.S.C. § 1343 and bank fraud, 18 U.S.C. § 1344.

121. The members of the Citadel Racketeering Enterprise share the common purpose of developing and operating a global credential stealing botnet operation as set forth in detail

above.

122. Defendants have knowingly and with intent to defraud used a counterfeit access device in the form of a Windows XP product key to install and activate an unauthorized copy of Windows XP in order to produce the necessary Citadel botnet software operated by Defendants. As set forth in detail above, Defendants have used the counterfeit access code to install and activate numerous unauthorized copies of Windows XP in order to establish a common programmatic environment so that other Defendants can craft and compile the necessary Citadel botnet software for use in the Citadel botnet, and in furtherance of their common financial goal of obtaining unauthorized access devices, all in violation of 18 U.S.C. § 1029(a)(1).

123. Defendants 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 Botnets created and operated by Defendants. As set forth in detail above, Defendants have used the Citadel Botnets to 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, all in violation of 18 U.S.C. § 1029(a)(2).

124. Defendants have also knowingly and with intent to defraud, possessed, and do possess, thousands of unauthorized access devices fraudulently obtained as described above, in violation of 18 U.S.C. § 1029(a)(3).

125. Defendants have also knowingly and with intent to defraud effected transactions with stolen unauthorized access devices to receive millions of dollars in payment from individuals' bank accounts, in violation of 18 U.S.C. § 1029(a)(7).

126. Also as set forth in detail above, Defendants have executed a scheme to defraud

scores of financial institutions by enabling members of the Citadel Enterprise to fraudulently represent themselves as bank customers, thereby enabling them to access and steal funds from those customer accounts, all in violation of 18 U.S.C. § 1344.

127. Each of the violations of 18 U.S.C. §1029(a) and 18 U.S.C. § 1344 described above were conducted using internet communications “transmitted by means of wire ... in interstate or foreign commerce,” in violation of 18 U.S.C. § 1343.

128. Microsoft has been and continues to be directly injured by Defendants’ conduct. But-for the alleged pattern of racketeering activity, Microsoft would not have incurred damages.

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

EIGHTH CLAIM FOR RELIEF

Conspiracy to Violate the Racketeer Influenced and Corrupt Organizations Act (RICO) – 18 U.S.C. § 1962(d)

130. Microsoft realleges and incorporates by reference the allegations contained in paragraphs 1 through 129 above.

131. Beginning during or before January of 2012 and continuing up through the filing of this Complaint, Defendants John Does 1 through 82 conspired to associate in fact with the Citadel Racketeering Enterprise and conduct its affairs through a pattern of racketeering activity, with such conduct and activities affecting interstate and foreign commerce. Defendants further conspired to engage in an unlawful pattern of racketeering activity involving thousands of predicate acts of fraud and related activity in connection with access devices, 18 U.S.C. § 1029, wire fraud, 18 U.S.C. § 1343, and bank fraud, 18 U.S.C. § 1344.

132. The members of the Citadel Racketeering Enterprise conspired for the common purpose of developing and operating a global credential stealing botnet operation as set forth in

detail above.

133. Microsoft has been and continues to be directly injured by Defendants' conduct. But-for the alleged conspiracy to conduct a pattern of racketeering activity, Microsoft would not have incurred damages.

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

NINTH CLAIM FOR RELIEF

Computer Trespass (North Carolina General Statutes § 14-458)

135. Microsoft realleges and incorporates by reference the allegations contained in paragraphs 1 through 134 above.

136. Defendants have interfered with, unlawfully and without authorization, and dispossessed Microsoft's personal property.

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

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

139. Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to alter or erase computer data, computer programs or computer software.

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

141. Defendants' actions in operating the Citadel Botnets result in unauthorized access

to Microsoft's Windows operating system and Internet Explorer software and the computers on which it runs, results in unauthorized intrusion into those computers, theft of information, account credentials and funds, and unsolicited, bulk electronic mail being sent to, from or through the computers of Microsoft.

142. Upon information and belief, Defendants intentionally caused this conduct and this conduct was unlawful and unauthorized.

143. Defendants' actions have caused injury to Microsoft, including time, money and a burden on the computers of Microsoft. Defendants' actions have caused injury to Microsoft's business goodwill and have diminished the value of Microsoft's possessory interest in its Windows operating system, Internet Explorer software, computers and software.

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

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

146. Defendants' actions violate North Carolina General Statutes §14-458(a)(1), (2), (3) and (4).

TENTH CLAIM FOR RELIEF

Conversion

147. Microsoft realleges and incorporates by reference the allegations contained in paragraphs 1 through 146 above.

148. Defendants have willfully interfered with, assumed, and exercised the right of ownership over the personal property of Microsoft, without authorization or justification, altering the condition of their property, as a result of which Microsoft has been deprived of possession

and use of its property.

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

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

ELEVENTH CLAIM FOR RELIEF

Unjust Enrichment

151. Microsoft realleges and incorporates by reference the allegations contained in paragraphs 1 through 150 above.

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

153. Defendants accessed, without authorization, Microsoft's Windows operating system and Internet Explorer browser and the computers running that software, which otherwise belong to Microsoft or its customers.

154. Defendants used, without authorization or license, the facilities, software and computers of Microsoft, which belong to Microsoft to, to among other acts, deliver malicious software, steal personal information, account credentials and money, support the Citadel Botnets, infringe the trademarks of Microsoft and deliver unsolicited, bulk e-mail and deceive users.

155. Defendants' actions in operating the Citadel Botnets result in unauthorized access to Microsoft's Windows operating system, Internet Explorer browser and the computers running that software, result in delivery of malicious software, theft of personal information, account credentials and money, support of the Citadel Botnets, infringement of the trademarks of

Microsoft, delivery of unsolicited bulk e-mail and deception of users.

156. Defendants profited unjustly from their unauthorized and unlicensed use of Microsoft's Windows operating system, Internet Explorer browser, software computers, and/or intellectual property.

157. Upon information and belief, Defendants had an appreciation and knowledge of the benefit they derived from their unauthorized and unlicensed use of Microsoft's Windows operating system, Internet Explorer browser, software, computers and/or intellectual property.

158. Retention by the Defendants of the profits they derived from their unauthorized and unlicensed use of Microsoft's Windows operating system, Internet Explorer browser, software computers, and/or intellectual property would be inequitable.

159. Defendants' unauthorized and unlicensed use of Microsoft's Windows operating system, Internet Explorer browser, software computers, and/or intellectual property has damaged Microsoft.

160. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial, and Defendants should disgorge their ill-gotten profits.

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

TWELFTH CLAIM FOR RELIEF

Nuisance

162. Microsoft realleges and incorporates by reference the allegations contained in paragraphs 1 through 161 above.

163. Defendants have made an improper use of their own property, the property of Microsoft and the property of Microsoft's customers in that way injures the property rights of

Microsoft.

164. Upon information and belief, Defendants' acts were intentional and unreasonable.

165. Defendants, operating software within Microsoft's Windows operating system and Internet Explorer browser, and 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.

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

167. As a direct result of Defendants' actions, Microsoft has suffered and continue to suffer irreparable harm for which it has no adequate remedy at law, and which will continue unless Defendants' actions are enjoined and unless the nuisance is abated.

PRAYER FOR RELIEF

WHEREFORE, Microsoft prays that the Court:

1. Enter judgment in favor of Microsoft and against the Defendants.
2. Declare that Defendants' conduct has been willful and that Defendants have acted with fraud, malice and oppression.
3. Enter a preliminary and permanent injunction enjoining Defendants and their officers, directors, principals, agents, servants, employees, successors, and assigns, and all persons and entities in active concert or participation with them, from engaging in any of the activity complained of herein or from causing any of the injury complained of herein and from assisting, aiding or abetting any other person or business entity in engaging in or performing any of the activity complained of herein or from causing any of the injury complained of herein.

4. Enter a preliminary and permanent injunction isolating and securing the botnet infrastructure, including the software operating from and through the Harmful Domains and IP Addresses and placing that infrastructure outside of the control of Defendants or their representatives or agents.

5. Enter judgment awarding Microsoft actual damages from Defendants adequate to compensate Microsoft for Defendants' activity complained of herein and for any injury complained of herein, including but not limited to interest and costs, in an amount to be proven at trial.


6. Enter judgment in favor of Microsoft, disgorging Defendants' profits.

7. Enter judgment in favor of Microsoft, awarding enhanced, exemplary and special damages, in an amount to be proved at trial.

8. Enter judgment in favor of Microsoft awarding attorneys' fees and costs, and;

9. Order such other relief that the Court deems just and reasonable.

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