IN THE UNITED STATES DISTRICT COURT

FOR THE WESTERN DISTRICT OF NORTH CAROLINA

CHARLOTTE DIVISION

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

I, Vishant Patel, declare as follows:

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

I. INTRODUCTION

A. My Experience In The Investigation Of Cybercrime

2. I have been a member of the Digital Crimes Units since August 2012. In my role on the Digital Crimes Unit, I assess security threats to Microsoft and the impact of such threats on Microsoft's customers and business. As a regular part of my duties, I work with other

investigators at Microsoft or from other institutions, such as financial institutions or government agencies, to analyze the technologies and strategies deployed by cybercriminals in a variety of settings, including financial theft and fraud.

3. Prior to my current role, I worked as a Senior Investigator, dealing with cyber threats. Among my responsibilities were responding and investigating to phishing attacks, malware, and system and network incidents. Before joining Microsoft, I worked for Citigroup Inc. A true and correct copy of my current *curricula vitae* is attached hereto as Exhibit 1.

B. Overview Of My Investigation Into Citadel And My Top Conclusions

4. I have investigated and continue to investigate the Internet activities of a group of cybercriminals who, among other illegal acts, break into and take control of the computers of end-users around the world, steal their financial credentials, and then use this information to pilfer their bank accounts. These criminals conduct their activities silently over the Internet. The primary means by which these cybercriminals operate is through what is commonly referred to as the "Citadel botnet."

5. A "botnet" is a network of end-user computers that have been infected with a particular type of malicious software ("malware"). This malware places the infected computers under the control of the individuals who operate the botnet. These botnet operators communicate with the infected computers over the Internet and use them to conduct their illegal acts. "Citadel" is a recently-emerged but highly sophisticated botnet designed to steal money from the financial accounts of the individuals whose computers have become infected with the Citadel malware.

6. As part of this investigation, I have conducted my own examination of the software used in the Citadel botnet, researched the criminal activities related to Citadel, and studied the infrastructure and business-model behind Citadel. I have also reviewed research

published or privately sent to me by other security researchers regarding the code, architecture and features of Citadel, including the command and control mechanisms, propagation methods, and use of the infected end-user computers that are part of the botnet. I have also consulted and worked with some of the leading security researchers for major financial institutions around the world who have also been studying the rapid and alarming spread of Citadel.

7. Based on this research and analysis, I have reached the following conclusions regarding Citadel. Citadel is an extremely sophisticated financial fraud botnet. It has been created by a Defendant, most likely operating out of the Ukraine or Russia. This Defendant has sold Citadel "builder kits" to other cybercriminals around the world. The term "builder kit" refers to a software package that allows someone to generate other software. Typically, the Citadel Builder Kit allows the purchaser to select various options that customize the configuration of their own Citadel botnet. After the options have been selected, the purchaser can literally push a "Build Bot" button, and the builder kit creates the executable modules and configuration files necessary to infect end-user computers with Citadel bot code. Each of these customers uses the builder kit, in combination with a stolen version of Windows XP and a stolen product key for Windows XP, both also provided by the vendor of the Citadel Builder Kit, to create, deploy, and operate one or more Citadel botnets used to commit crimes in a particular region or territory.

8. The Defendant who develops and commercializes the Citadel Builder Kit has gained distinction among cybercriminals by providing an unusual degree of after-sales service to Citadel Builder Kit customers. Using a customer relationship management interface ("the Citadel CRM") set up by the developer of Citadel, the Citadel botnet operators can contact the developer and each other for updates to Citadel code; support with technical problems; and best

practices in deploying, running, and defending a botnet. Additionally, using the Citadel CRM, the developer of Citadel solicits or proposes new feature ideas from or to customers, and the customers can vote on which feature or features they would like to see implemented, and even bid what price they would offer the Citadel developer to implement the feature.

9. In short, my investigation has uncovered what is, in effect, a Citadel enterprise, comprised of a defendant who develops, commercializes, and supports the Citadel Builder Kits, cooperating with and supporting defendants who have purchased the builder kits and who have created and deployed one or more Citadel botnets. All of these Defendants continue to cooperate with one another to further their shared criminal ends.

10. Citadel inflicts extreme damage on individuals whose computers have been infected by Citadel. 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. Additionally, Citadel inflicts extreme damage on 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.

11. Further, Citadel inflicts extreme damage on Microsoft by creating and deploying malware specifically designed to attack computers running Microsoft software. Microsoft's brand, trademarks, reputation, and customer goodwill are all damaged by Citadel. In addition, Microsoft must deploy significant resources to help its customers defend themselves against Citadel.

12. I am joined in these conclusions by the other security professionals who have been studying Citadel with whom I have been consulting.

C. Outline Of My Declaration

13. In the remainder of this Declaration, I will explain the following topics:

a. The organization and structure of the Citadel botnet;

b. The criminal activity engaged in by the Defendants using the Citadel botnet and the resultant harms to Microsoft, Microsoft's customers and third parties, such as financial institutions, NACHA and other organizations impacted by the Defendants;

c. The manner in which the Citadel botnet has been commercialized and deployed around the world by cybercriminal organizations;

d. The harms caused by the Defendants through their use of Citadel to Microsoft, owners of infected computers, the banking industry and NACHA;

e. The manner in which Microsoft can disrupt and significantly curtail the criminal activities perpetrated by Defendants through Citadel.

II. CITADEL—STRUCTURE AND FUNCTION OF A CRIMINAL BOTNET

A. Botnets In General

14. As I stated above, a botnet is a network made up of end-user computers connected to the Internet that have been infected with a certain type of malicious software ("malware"). The malware places the infected computers under the control of individuals or organizations running the botnet who utilize the infected end-user computers to conduct illegal activity. For the remainder of this Declaration, I will refer to the Citadel botnet malware running on the end-user's infected computer as a "Citadel bot" or simply a "bot," and the network made up of the separate bots as a "Citadel botnet."

15. A botnet network may be comprised of as few as hundreds or as many as tens of

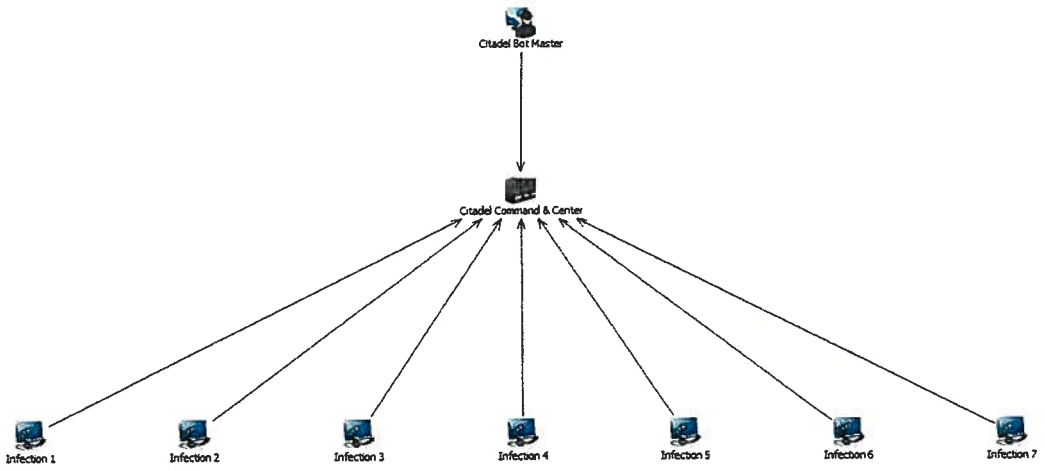
thousands or millions of bots running on infected end-user computers. Once a large-scale botnet has been created, its massive infrastructure can be used by the botnet operators to engage in illegal activity—such as stealing financial credentials, stealing personal identification information, stealing confidential data, sending spam email or anonymously carrying out other technical activities or attacks.

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

16. Citadel is a financial-fraud botnet. The primary aim of Citadel is to infect end-user computers in order to (1) steal credentials for online accounts, such as account login information for bank or other financial account credentials, from the owners or users of those computers; (2) access the victims' online accounts with the stolen credentials; and (3) transfer information or funds from the victims' accounts to accounts or computers controlled by the Defendants.

17. 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 can be represented as shown in Figure 1, below:

Fig. 1

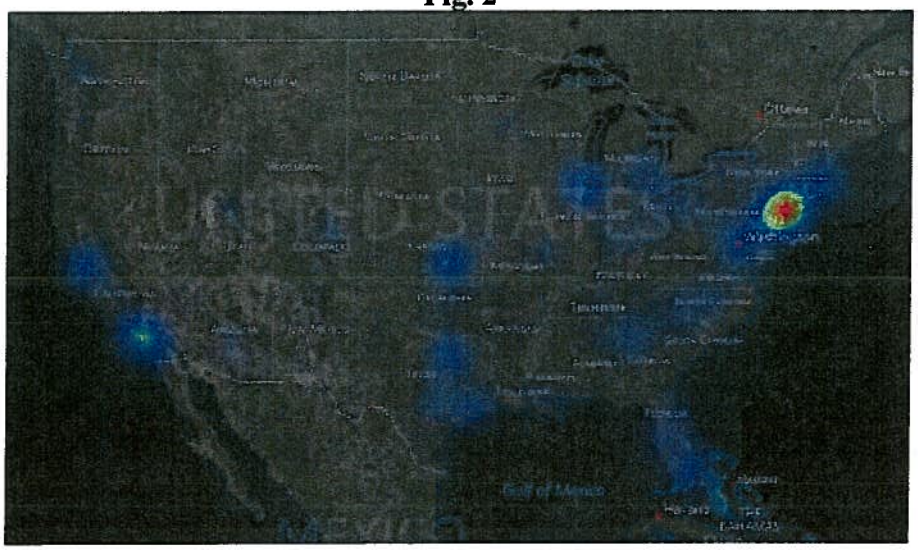


1. The Citadel Infection Tier

18. Across the Citadel botnet enterprise, the infection tier consists of an estimated two to five million bots running on infected end-user computers. This is based on evidence showing there are at least 1300 Citadel botnets, with an average size of 3,500 infected computers in each. These end-user computers are of the type commonly found in businesses, living rooms, schools, libraries, and Internet cafes around the world. I refer to this tier as the "Infection Tier" of the Citadel botnets. Defendants target the owners of computers in the infection tier and steal financial account credentials and other personal information from them. Theft attributed to Citadel operators has been estimated to be in the millions of dollars.

19. Computers that Defendants have targeted for infection by Citadel can be found in every state in the United States and in almost every corner of the world. For example, Microsoft has been able to locate Citadel bots running on infected end-user computers in the United States. Figure 2, below, shows the concentrations of these bots. Green signifies a higher concentration of infected computers than blue, and red signifies the highest concentration.

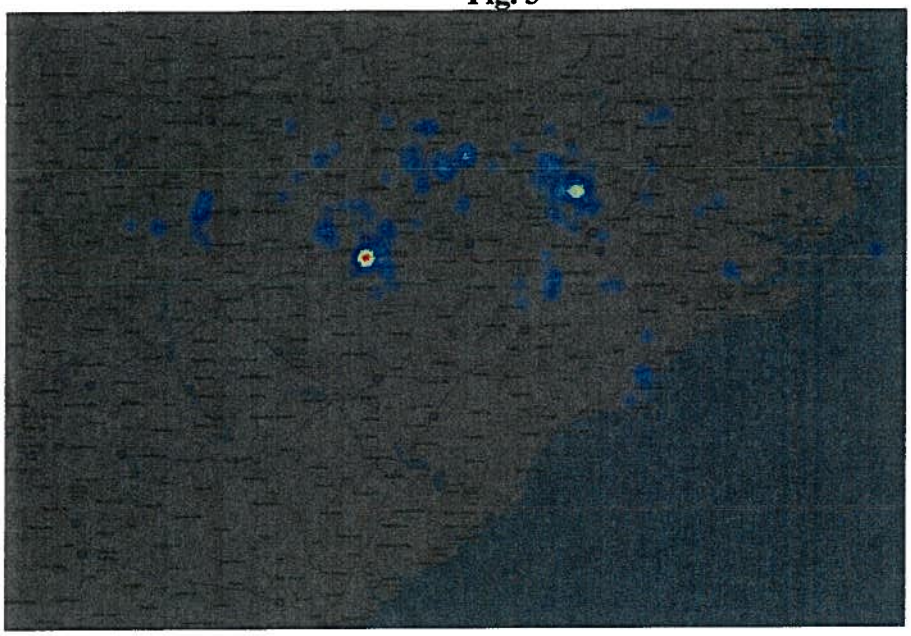
Fig. 2



20. Figure 3, below, shows the locations of some of the Citadel-infected computers,

believed to be located in the North Carolina, based on an analysis of IP addresses through which those computers are connecting to the Internet, as uncovered during my investigation. The greatest concentration of these is located in Charlotte.

Fig. 3



2. <u>The Citadel Command and Control Tier</u>

21. 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.

22. Each Citadel bot running on an infected end-user computer is programmed to periodically connect over the Internet to one or more command and control servers. 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 bots on infected end-user computers.

23. I have observed that Citadel bots attempt to contact command and control servers every 20 minutes. Thus, the botnet operators have the ability to communicate with the bots on infected end-user computers almost instantaneously. Servers in the Command and Control Tier include the servers at the domain names and IP addresses at Exhibits 2 and 3, which are described more fully below.

24. A "domain name" (commonly thought of as a website name) is an alphanumeric string separated by periods, such as "bestchoiceininvest.com." Each domain name that is active (i.e., registered and operative on the Internet) maps to a numeric IP address, which indicates the physical address of the computer connected to the Internet hosting the domain. An "IP address" is a unique string of numbers separated by periods, such as "149.154.152.161" that identifies each computer connected to the Internet. Part of the infrastructure of the Internet maps domain names to IP addresses. Each active domain name on the Internet has a corresponding IP address at which the website content is located.

25. The Defendants control the domain names and IP addresses that are used to distribute and propagate the botnet code, to receive communications from the bots, and to control the bots. True and correct lists of these malicious Citadel botnet domain names and IP addresses are attached as Exhibits 2 and 3 to this declaration. These will be explained in greater detail in the following section of this Declaration. The relief sought in this case is directed at disabling all Citadel botnets that make up the Citadel enterprise by taking control of these domain names and IP addresses through which the Defendants control the Citadel bots running on infected end-user computers.

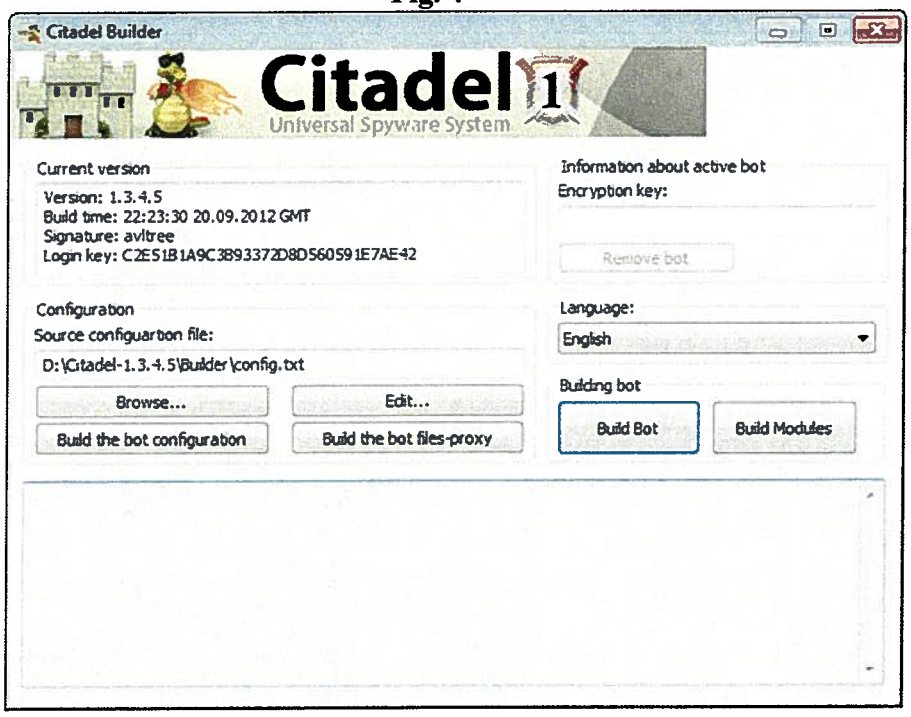
III. CREATION, PROPAGATION AND OPERATION OF CITADEL BOTNETS

A. Creation Of Citadel Botnet Code And Configuration Files

26. As I noted in my Introduction, to create a Citadel botnet, a Defendant begins by

purchasing a builder kit ("Citadel Builder Kit") from the creator of Citadel. Evidence suggests that, as of early 2012, a Citadel Builder Kit cost approximately $2400, with a monthly "rent" fee of $125, not including add-on modules or updates, which were extra. The builder kit is a software application that walks 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 (a.k.a. "the bot") that will infect and control end-user computers, as well as configuration files that the botnet operator will place on command and control servers so as to send instructions to the bots on the end-user computers. Figure 4, below, shows a screen shot taken from a Citadel Builder Kit.

Fig. 4



27. One of the important aspects of the Citadel enterprise is the level of support offered by the Defendant who develops and commercializes Citadel. To control the costs of support, this Defendant urges 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 the Citadel developer to test the Citadel Builder Kits.

28. In order to provide his botnet customers with access to Windows XP without having to pay Microsoft for it, the vendor of the Citadel Builder Kit provides a stolen version of Windows XP and a unauthorized product key for Windows XP. Figure 5, below, shows a section taken from the Citadel Builder Kit manual. It gives Citadel customers a path (no longer active) to a version of Windows XP, and it provides, in red, an unauthorized product key for that copy of Window XP.

Fig. 5

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

B. Creation Of Citadel Command And Control Infrastructure

29. 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 relatively easily 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. Many webhosting companies in the United States, for example, offer secure, climate controlled, professionally run facilities where rows

upon rows of computers are connected 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.

30. In previous investigations of other botnets, I and other Microsoft investigators have found that, almost without exception, these webhost accounts are set up using false identification information and are often paid for using anonymous means or through stolen credit cards. Often, a webhost in the United States will sell excess capacity through resellers located in other regions of the world. For example, I have seen instances where a botnet operator has leased capacity from a webhost reseller in Azerbaijan, who is reselling capacity for a webhost located in the United States. These levels add complexity to the command and control tier and hence allow the botnet operators to operate with greater anonymity.

31. The most vulnerable point in the Citadel botnet architecture are the domain names and IP addresses of the command and control servers, as they can be identified and, if 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. However, as discussed further below, Citadel botnets have many built-in defensive mechanisms that will need to be overcome before Citadel can be neutralized as a threat.

C. Propagation And Control Of Citadel Botnets

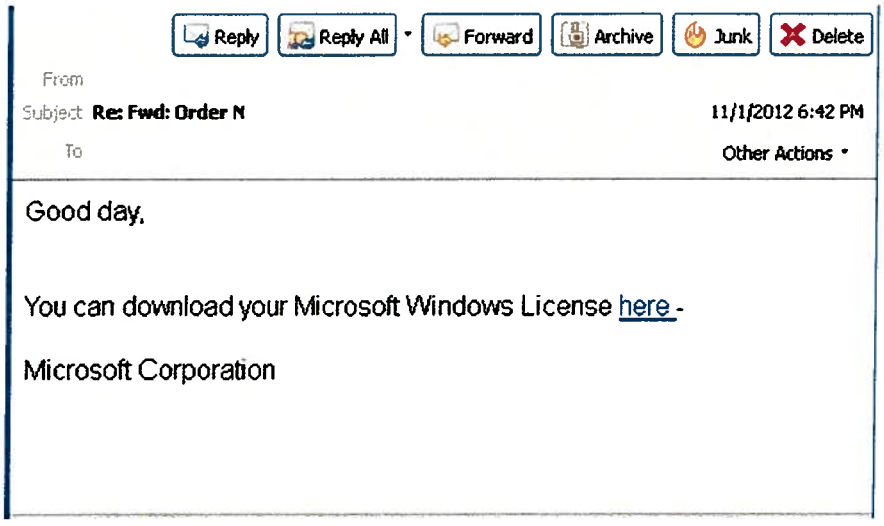
1. Spam Is Used To Lure End-Users To Attack Websites

32. The Defendants use several methods to infect end-user computers. 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. 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. Attached hereto as Exhibit 4, is a true and correct copy of an article describing a recent hack of the website of a major United States press organization, in which Citadel botnet operators staged a download kit on the organizations website. This demonstrates the pervasive nature of Citadel and the brazenness of Citadel botnet operators.

33. 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 volume of such spam is significant, particularly directed to Microsoft's Outlook.com, Hotmail and other email services and place a severe burden on those servers. 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. These spam emails include links that, when clicked, direct the user to one of the infection domains or IP addresses, and results in the infection of the user's computer with the malicious software. Figure 6, below, shows true and correct examples such spam, with the intended victim's e-mail address redacted. Such emails have been seen, for example, to download the Blackhole exploit kit, which then delivers Citadel malware:

Fig. 6



From: "NACHA - The Electronic Payments Association" <marketing@nacha.org>
Date: April 16, 2013, 1:13:52 PM EDT
To: <[redacted]@[redacted].com>
Subject: Rejected ACH payment

Rejected ACH payment

The ACH process (ID: 8818190842563), recently sent from your checking account (by one of your account members), was canceled by the recepient's bank.

More details

Declined transfer	
Transaction ID	8818190842563
Reason of request abort	Review more info in the statement below
Transaction Detailed Report	report_8818190842563.doc (Microsoft Word Document)

Find more information and status updates here

NACHA - The Electronic Payments Association
13450 Sunrise Valley Drive, Suite 100, Herndon, VA 20171
Ph: 703-561-1100 | Fx: 703-787-0996 | info@nacha.org
www.nacha.org

Unsubscribe here.

13450 Sunrise Valley Drive, Suite 100, Herndon, VA 20171

NACHA does not send communications of any type to persons or organizations about individual ACH transactions that they originate or receive. If you or your customer has received a communication of this nature thatpurports to come from NACHA, it is fraudulent. Visit NACHA's website at nacha.org for more industry information on fraud, email phishing, and corporate account takeover including resources from the FDIC and the FTC. NACHA does not sell or release email addresses.

34. It can be seen that the Citadel botnet operators misuse the trademarks of well known companies and organization such as NACHA to fool the recipient into thinking the spam e-mail is from a legitimate source.

2. Exploit Packs Download Citadel To Vulnerable Computers

35. Once an end-user connects to the website, where a specialize and highly sophisticated piece of software known as an "exploit pack" will be staged, the 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, an unpatched application. If a vulnerability is found, the exploit pack will cause the download of the Citadel 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. They are, in fact, converted into weapons of crime aimed directly at the end-user's bank accounts.

3. The Newly Installed Citadel Bot Reaches Out To Base Domains For Configuration Files

36. Once 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. They are hard-coded into the bot's code when it is built, which means the base addresses are an integral part of the Citadel bot executable. But studying many thousands of Citadel bots, I have developed a list of base domains. A true and correct list of such Citadel base domains is attached hereto as Exhibit 5.

4. Information In The Configuration Files Control The Bot's Activities

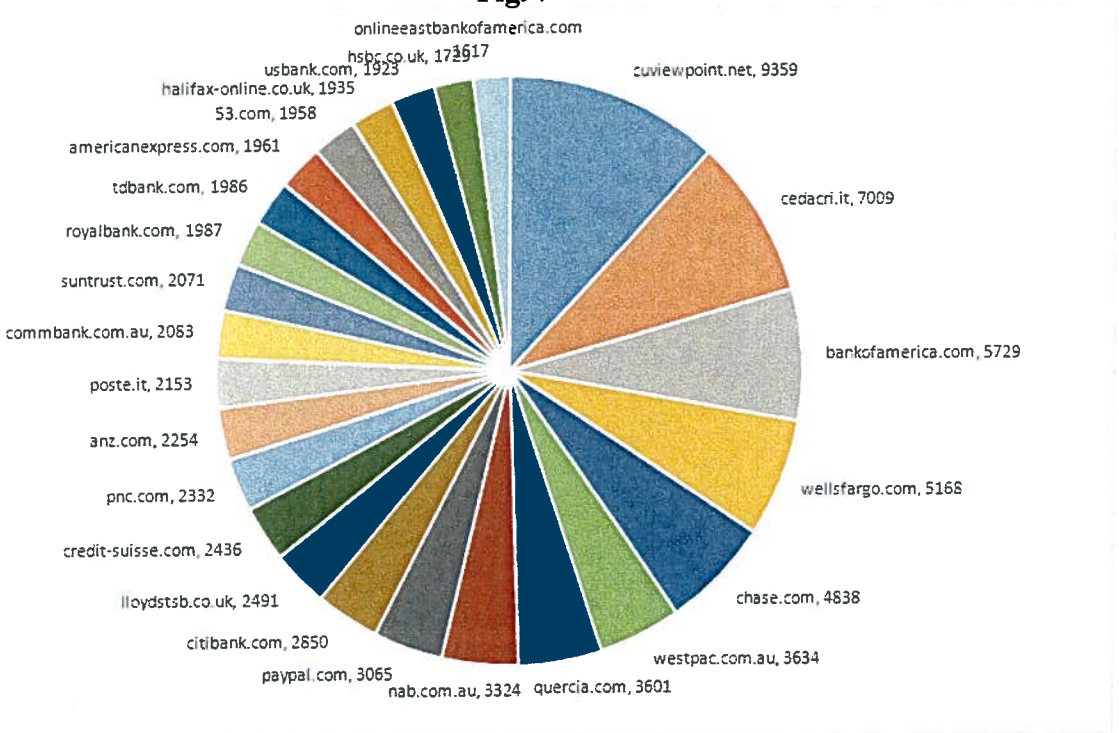
37. Once a Citadel bot (the Citadel code infecting and controlling an end-user computer) establishes contact with one of these base domains, the bot will download a configuration file from it. Citadel configuration files are encrypted text files. They contain various types of information which will control 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. The domains listed in Exhibit 6 host the Citadel configuration files. Exhibit 7 is an excerpt of an unencrypted Citadel configuration file.

38. By monitoring infected computers, we have been able to capture the information contained in samples of the encrypted configuration files. A number of sections are noteworthy. First, configuration files contain 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. By studying many configuration files, I have been able to develop a list of the financial institutions attacked by the various Citadel botnets in operation. A true and correct copy of this list is attached hereto as Exhibit 8.

39. Moreover, I have developed data on how often particular banking institutions are targeted by Citadel. Figure 7, below, is a pie chart showing the number of times each of the top 25 Citadel targets has been listed in a captured configuration file. 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.

Fig. 7



40. Attached hereto as Exhibit 9 is a complete and correct list of all of the financial institutions that I have found targeted in Citadel configuration files, along with the number of time I have seen each institution mentioned.

41. 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. Exhibit 2 contains a true and correct list of Citadel Command and Control servers of this type.

42. Additionally, a Citadel configuration file will contain a list of websites from which an end-user might attempt to download anti-virus software. The Citadel bot detects when the end-user attempts such a connection, and redirects the user to another website. This is a defensive mechanism meant to keep the user from detecting or expunging the Citadel bot running on their computer. Exhibit 10, attached hereto, contains a list of the over 1200 websites that a Citadel bot will keep an end-user from connecting to in order to block the end-user's attempt to download anti-virus software or to patch their computer.

43. Further, a Citadel configuration file will contain a list of software applications that security investigators often use while studying an infected computer. The bot will assess all other applications running on the same computer. If it detects the presence of any of these common investigative tools, it will alter its behavior. This is also discussed in more detail below. Exhibit 11, attached hereto, contains a report by a security researcher regarding this aspect of the Citadel configuration file.

44. Additionally, a Citadel configuration file will contain information that the bot will use to keep from attacking end-users or financial institutions in particular countries. For example, the Citadel "License Agreement" is in the Russian language and Paragraph 2 of that document includes the statement "the product will not work on systems with the Russian and

Ukrainian layout." A true and correct copy of the original License Agreement is attached as Exhibit 12. 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 them.

D. Defensive Mechanisms Of Citadel Botnets

45. I have observed that certain features of the command and control infrastructure enable Citadel botnets to better withstand technical counter-measures.

46. The first defensive mechanism is the migration, over time, of the command and control infrastructure. Under normal circumstances, the set of domains and IP addresses associated with the Trojan downloader and Blackhole exploit kit changes every 7-10 days. The command and control servers that the installed bots communicate with are changed more gradually, but there is generally a complete turnover every six to eight weeks. Certain domains and IP addresses fall out of use by the bots and the Defendants. New domains and IP addresses are added to those that bots communicate with. In essence, the set of domains and IP addresses used in the command and control infrastructure is a dynamic, moving target, making attempts to disable the botnet by attacking the Command and Control tier more challenging.

47. The second defensive mechanism 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. As noted above, when the Citadel code first infects a user's computer, it is programmed to contact one to five computers on the Internet from which it will attempt to download a configuration file. The configuration file will contain a new and generally longer list of domains on the Internet with which the infected end-user computer will now communicate. Because the bots check for a new configuration file every 20 minutes, by changing the configuration files, the botnet operators are able to quickly update the set of command and

control domains through which they control the infected end-user computers. This means that the botnet operators will be able to shift the infected computers over to a new set of command and control servers very quickly if they detect an attack has started on the existing command and control infrastructure.

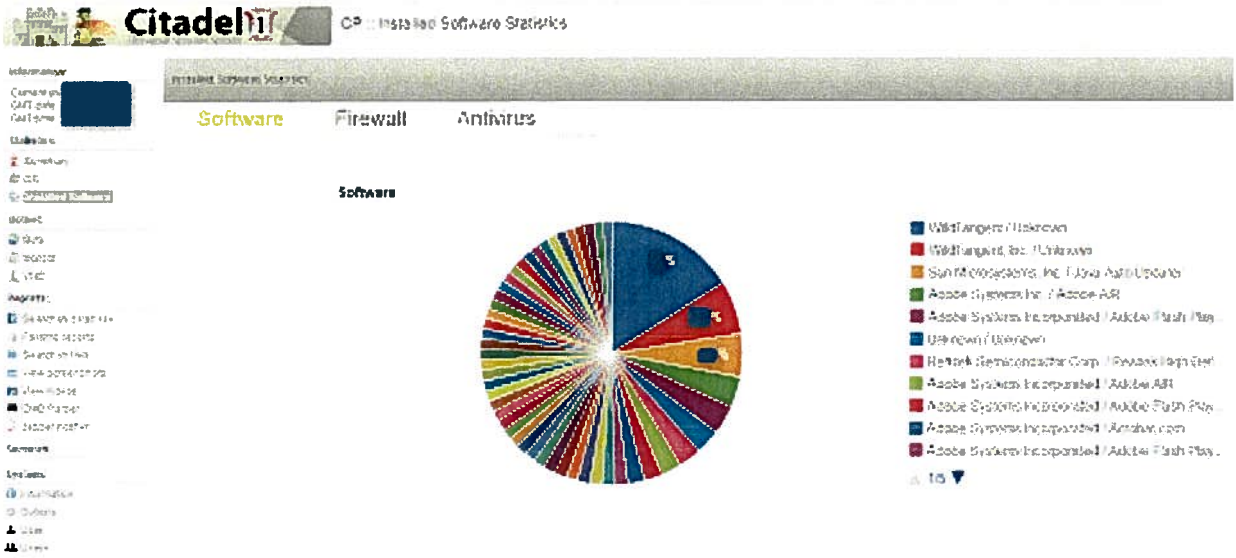
48. The third defensive mechanism is the use of encryption. In most versions of the botnets, communications between the infected end-user computers and the command and control servers are encrypted. This includes both the configuration files downloaded by the bots, and the stolen information uploaded by the bots. Over time, and in reaction to advances made by researchers attempting to defend against Citadel, Citadel has deployed increasing sophisticated encryption. Specifically, in response to published reports on how Citadel used the RC4 encryption algorithm to encrypt data, Citadel's authors changed Citadel's encryption routines to use a more robust and secure 128-bit AES in addition to RC4 to encrypt its configuration file.

49. A fourth defensive mechanism is the ability of the Citadel bot to detect if it is being run on a computer being used by security researchers to study it. It is, for example, common for researchers to purposely infect computers with a bot so that the botnet code can be studied under laboratory conditions. The computers used to host these infections are usually configured with particular types of software that facilitate the study of the infection. If the Citadel bot detects that it is running on a computer that is also running the software commonly used in such security research settings, it will change its behavior. A Citadel bot does this by scanning every running process on the system. The bot then traces each running process to the original executable file and checks the company name and product name in the version information of each executable for strings such as "vmware," "geswall," "sandbox" "safespace," "bufferzone" or "virtualbox." If such software is detected, the Citadel bot will alter its behavior.

Rather than connecting to its normal command and control servers, the bot will generate a random "decoy" domain name and URL path for the command and control server and will attempt to connect to the non-existent command and control server. By using this approach, the Citadel bot gives the appearance of functioning normally. However, by attempting to contact a non-existent command and control server at an invalid URL instead of the legitimate command and control server, it seeks to lead investigators away from the actual command and control infrastructure.

50. A fifth defensive mechanism, noted above, is that the Citadel code running on the end-user computer will keep that computer from connecting to domains associated with anti-virus software. In other words, if a user attempts to connect to a website from which to download anti-virus software, Citadel will block that. Citadel does this through what is referred to as "DNS filtering." When the Citadel bot detects an attempt to connect to an antivirus website, it will hijack the session 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. Citadel botnet operators invest a great deal of care in studying the antivirus software arrayed against them. Figure 8, below, shows a screenshot from a Citadel botnet command interface, showing that the botnet operator is able to track all of the antivirus software running on the computers in the botnet.

Fig. 8



51. True and correct excerpts of a manual and configuration file addressing these defensive techniques are set forth as Exhibit 13. In summary, Citadel botnets are armed with a number of strong defensive mechanisms that make their analysis and disablement far more difficult and expensive than would otherwise be the case.

IV. CITADEL DAMAGES ITS VICTIMS IN MULTIPLE WAYS

A. Financial Fraud

52. The primary aim of Citadel botnet operators is to steal the financial account credentials belonging to the owners of the infected computers in order to access the end-user's bank accounts and siphon funds to the Defendants or other criminal organizations. Citadel botnet operators deploy, through Citadel, multiple tools and techniques to conduct this theft.

53. In general, a Citadel attack begins when the bot running on the infected end-user computer detects that the user is attempting to connect to the website of a financial institution. The bot determines this by checking the addresses to which a user is attempting to connect against a list of known financial institutions included in it configuration file.

54. 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 simply log the keystrokes entered by the user while the user logs in and 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 download and use it to attempt to steal from the user's accounts or conduct other illegal acts with the identification information stolen from the user.

55. In a more sophisticated 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. A true and correct sample of web inject code, extracted from a Citadel configuration file, is attached hereto as Exhibit 14.

56. For example, if the real website asks only for a login ID and password, the bot can extend it through a web-inject and ask for additional information such as social security number, birth date, mother's maiden name, and other such information typically used to answer security questions. Again, the Citadel bot will record this information and upload it later to the botnet operator, who can use it to steal from the end-user. Citadel is capable of exploiting various browsers in this manner including Microsoft Internet Explorer, Google Chrome, and Mozilla

Firefox.

57. In a still more sophisticated version of this attack, the Citadel bot can simply 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. 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. 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.

58. In a variant of this attack, instead of downloading a template for the website of the financial institution, the Citadel bot running on the end-user's computer can connect the user to a completely fake website controlled by the botnet operator that appears to be the website of the financial institution.

59. Our investigation has shown that Citadel botnet operators study the websites of the financial institutions they intend to target, and create web-inject code, website templates, or false websites carefully designed to mimic the real website. 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.

60. More sophisticated still, Citadel bots provide a built-in Virtual Network Console (VNC) server with the ability to connect out to a remote server. This feature allows the botnet operator to directly access the infected computer over the Internet, bypassing network address translation and firewall restrictions on inbound connections. From this point, the botnet operator can connect the 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.

61. Additionally, the Citadel bot can take static screenshot of a user's desktop or a "video" of the user's browsing session. This feature could be used to steal sensitive information such as account balances, or to acquire authentication information. The ability to capture these images allows a malicious actor to monitor portions of a victim's entire browsing session at a target of interest. This knowledge could be valuable to a malicious actor to better understand how an online banking application works. The video capture plugin is typically downloaded from the command and control server when the bot connects to it for the first time.

62. 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. Many aspects of the information gathering and the attacks can be automated by the botnet operator so that the bot code running on each end-user computer can advance the theft autonomously.

63. Figures 9 and 10, below, show two screen-shots of what an example Citadel "web

inject" 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.

Fig. 9

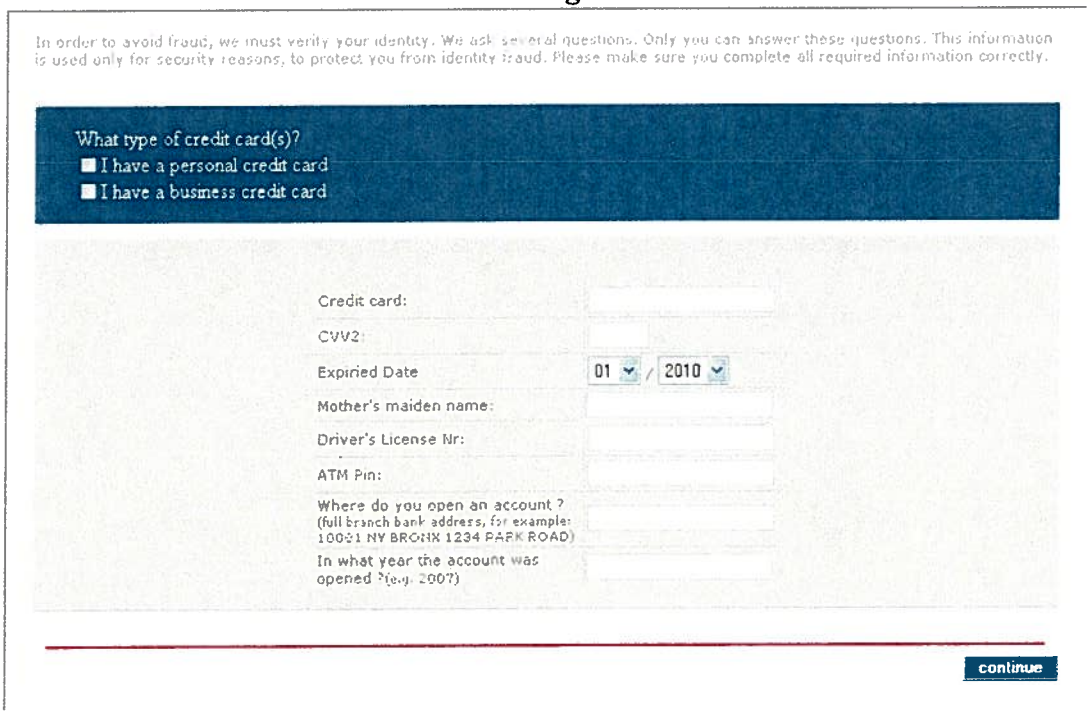
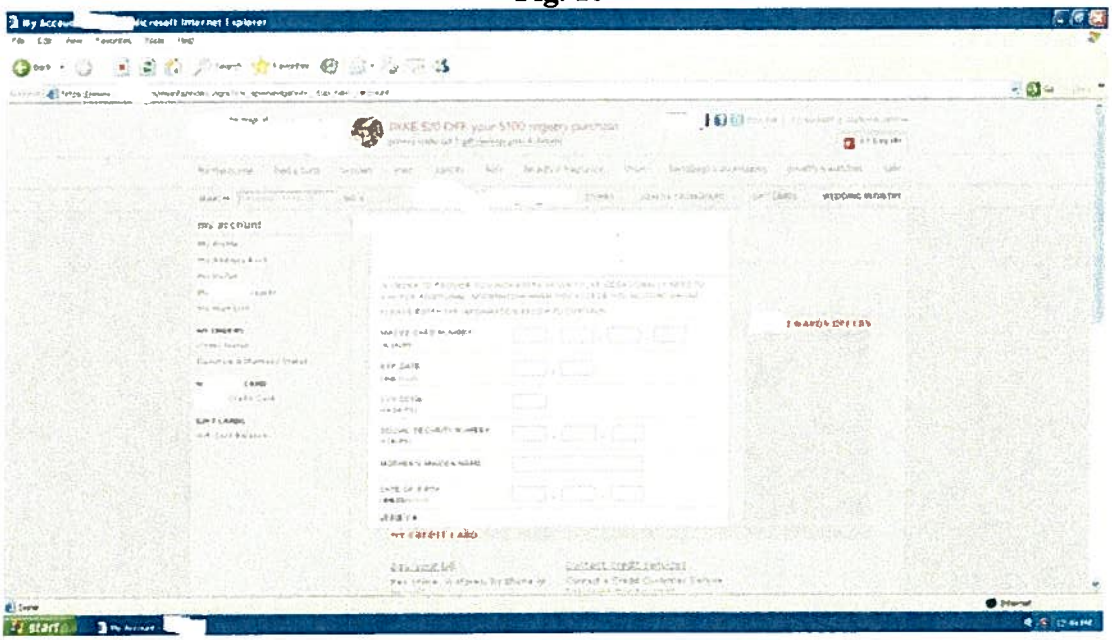
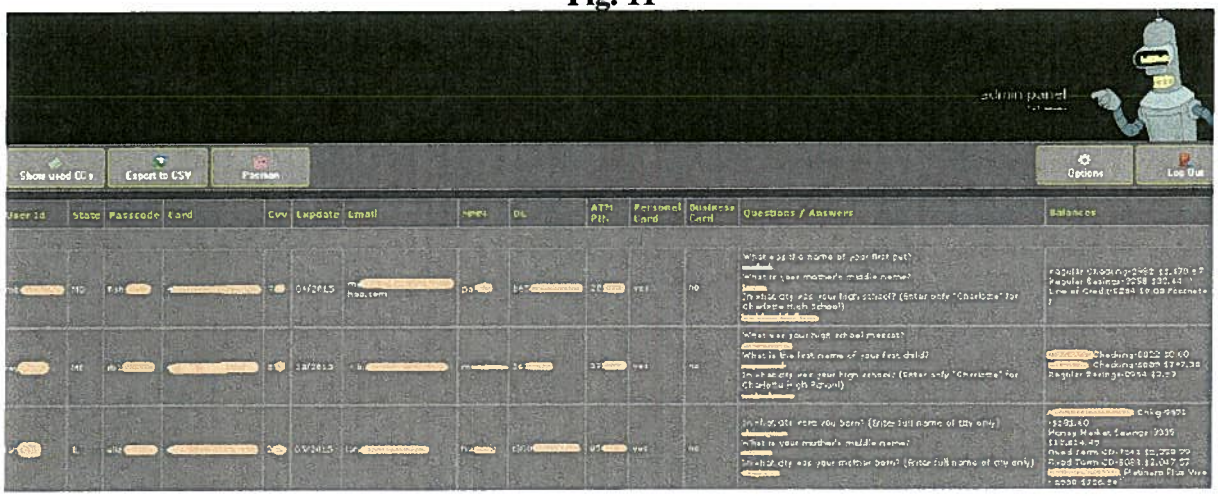


Fig. 10



64. Fig. 11, below, shows a Citadel console, used by the botnet operator to organize and display stolen credit card information and personally identifiable information. The excerpt has been redacted.

Fig. 11



B. Increased Likelihood Of Secondary Infections

65. 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. For example, Citadel bots have been associated with a type of malware known as "ransomware." Ransomware is a type of malware which locks the infected end-user computer until the owner of the computer pays a fee. Alternatively, it may encrypt files on the end-user computer until, again, the owner of the computer pays a fee.

66. The type of ransomware that Citadel bots have been seen to download is called "Reveton." Reveton attempts to scare a victim into sending money directly to the criminals. It may encrypt files on the victim's computer and demand that payment be sent in exchange for a decryption tool. Alternatively, it may trick victims into believing that they are the subject of a

law enforcement investigation, and that they must pay a fine to avoid further prosecution.

67. Reveton displays a window that covers the entire desktop and disables keyboard shortcuts for minimizing windows and displaying the Task Manager, making it extremely difficult to close. The victim is typically instructed to purchase an electronic payment card through services such as MoneyPak or Ukash. These cards can easily be purchased at local convenience stores, and they allow individuals to easily make electronic payments by providing a code from the card. Figure 12, below, shows a screen shot of a computer infected with Reveton ransomware.

Fig. 12

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

68. 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

69. 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. While the malicious software can infect a number of operating systems, the versions of the software targeted in this case are specifically designed to infect and run on computers equipped with the Windows operating system. The Windows operating system is licensed by Microsoft to end-users. Attached hereto as Exhibit 15 is a true and correct copy the Windows 7 end-user license agreement. Attached hereto as Exhibit 16 is a true and correct copy of the Windows Vista end-user license agreement. Attached hereto as Exhibit 17 is a true and correct copy of the Windows XP end-user license agreement.

70. The installation of malicious software in and of itself damages the user's computer and the Windows operating system on the user's computer. 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. For example, the Defendants create registry key paths

bearing the "Microsoft," "Windows" and "Internet Explorer" trademarks, within the Microsoft operating system, including the following:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\Microsoft\Internet Explorer\Privacy
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4
HKLM\\SOFTWARE\\Policies\\Google\\Update /v Update{8A69D345-D564-463C-AFF1-
A69D9E530F96} /t REG_DWORD /d 0
HKLM\SOFTWARE\Policies\Google\Update /v Update{8A69D345-D564-463C-AFF1-
A69D9E530F96} /t REG_DWORD /d 0
```

71. Citadel executes several commands upon infection. Some of the commands to gather additional information on the infected machine (Example: ipconfig, tasklist, net share, net view, hostname, netstat –a, ping www.eset.com, & net share). 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. In the following excerpt, such commands and changes are shown in red.

```
"""C:\Program Files\Microsoft Security Client\Setup.exe"" /x /s"
dir %windir%\system32\inetsrv\*.xml
hostname
ipconfig /all
net config workstation
"net localgroup ""Remote desktop users"" iis_admin /add"
net localgroup Administrators iis_admin /add
net share
net start TermService
net user
net user iis_admin Flvbyrj12 /add
net view
net view /domain
netsh firewall set opmode disable
```

```
netstat -a
"osql -E -Q ""exec sp_databases"""
osql -L
ping www.eset.com
REG ADD HKLM\\SOFTWARE\\Policies\\Google\\Update /v Update{8A69D345-D564-
463C-AFF1-A69D9E530F96} /t REG_DWORD /d 0
REG ADD HKLM\SOFTWARE\Policies\Google\Update /v Update{8A69D345-D564-463C-
AFF1-A69D9E530F96} /t REG_DWORD /d 0
set USERNAME && net localgroup Administrateurs
set USERNAME && net localgroup Administrators
tasklist
tasklist /V
```

72. Exhibit 13, attached hereto, also includes a true and correct listing of some of the commands that a bot executes on Windows immediately after being installed that cripple or overcome Windows security features. A true and correct copy of a report by security research firm Dell SecureWorks, describing Citadel's intrusion into the Windows operating system and browser software, and its defensive features, is attached as Exhibit 20. A true and correct copy of a document provided by John Doe 1 listing some of the commands that other Defendants may use to operate the botnet is attached as Exhibit 23.

73. 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.

74. 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. 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.

75. 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, as manual steps to remove the malicious software may be difficult for ordinary users. Attached as Exhibit 18 are true and correct copies of such manual procedures.

76. Even with professional assistance, cleaning an infected end-user computer can be exceedingly difficult, time-consuming, and frustrating. For example, attached as Exhibit 19 are true and correct copies of a small sample of customers' communications on Microsoft-run Internet forums and elsewhere related to instructions and attempts to identify and eradicate infections by the Citadel or the associated Reveton infection. These communications demonstrate the extreme problems that this infection creates for Microsoft's customers and the irreparable injury to both Microsoft and its customers. Microsoft and other members of the public must invest considerable time and resources investigating and remediating the Defendants' intrusion into these computers. Microsoft must spend time and resources to combat and remediate infections of user computers caused by the Citadel Botnets.

E. Citadel Causes Severe Injury To Microsoft

77. 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.

78. 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. Given the scale of this threat, Microsoft has had to invest significant resources attempting to clean these machines and counter this ever-evolving threat. Microsoft has had to constantly update its signature files for Citadel to counter the threat as Defendants means of evasion evolve.

79. I believe that 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.

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

80. As set forth more fully in the declarations of Pamela Moore, Eric Guerrino, William Johnson, and John Wilson, Citadel causes injury to numerous financial institutions, whose interests are represented by the trade groups NACHA, FS-ISAC and American Bankers Association, as well as Microsoft, and individual accountholder victims whose information and funds are stolen.

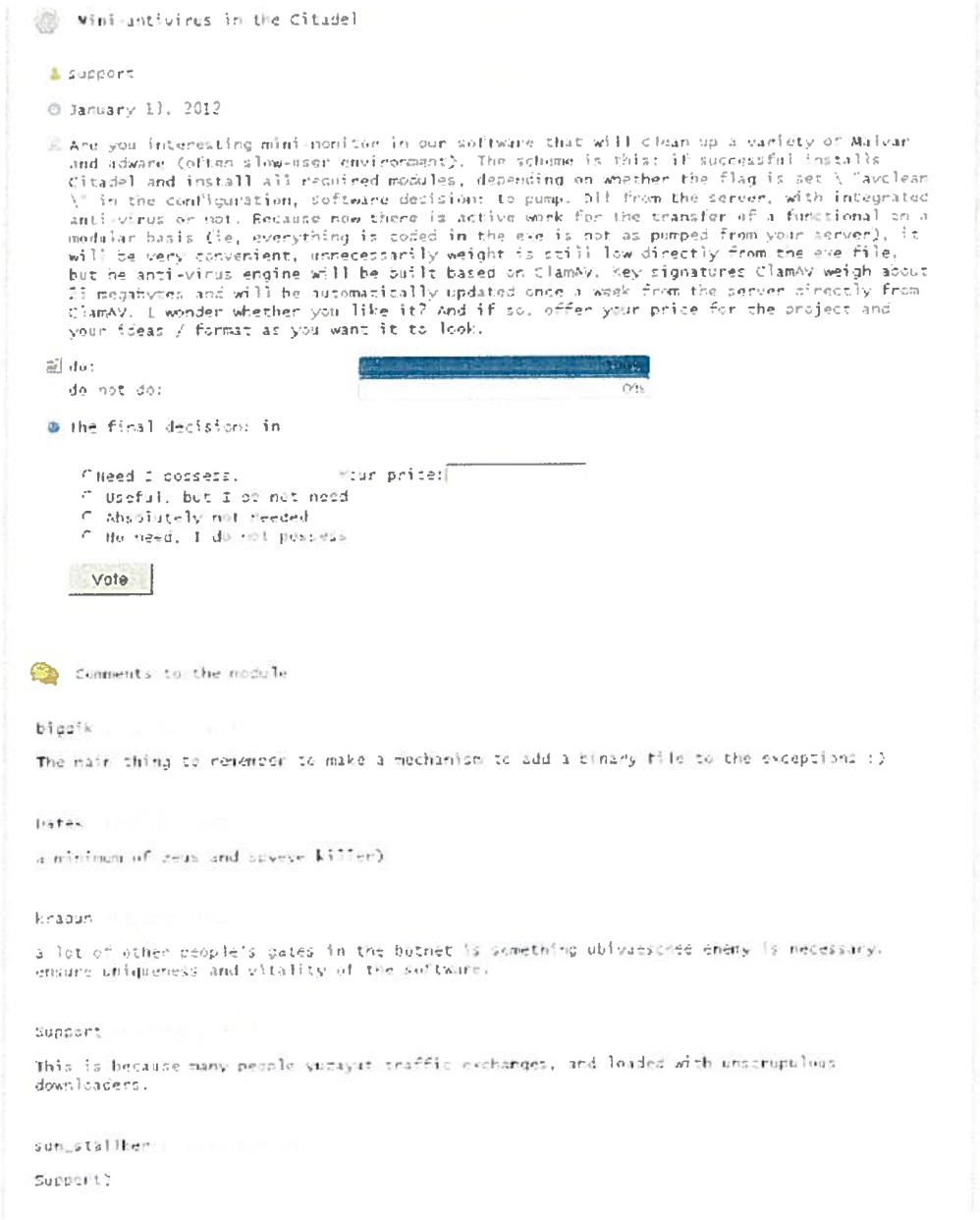
V. THE GLOBAL CYBERCRIME ENTERPRISE PROMOTING CITADEL

81. As explained above, Citadel is offered by Defendants as a "builder kit" that allow other cyber criminals to easily setup, operate, maintain, and propagate Citadel botnets to infect end-user computers, carry out theft of online credentials for financial institution websites, engage in financial theft, engage in identity theft, send spam email or engage in other malicious activities.

82. From its first public appearance in January 2012, one advantage of Citadel touted by the Defendant John Doe 1 who created and commercialized it is the promise of a high level of customer service. Attached as Exhibits 21 and 22 are true and correct copies of reports by security research Brian Krebs, discussing the high level of interaction and cooperation between Defendant John Doe 1 and Defendants who acquire and operate the Citadel Botnets. To deliver this customer service, this Defendant John Doe 1 provides an online portal called Citadel CRM (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. Figure 13, below, shows a screen shot of the Citadel CRM. The content of the screen

is consistent with the findings of my own investigation into Citadel.

Fig. 13



83. As can be seen from this dialog, the Defendant developing and commercializing Citadel proposed a new feature on January 13, 2012 and solicited the feedback of customers. The post includes a set of buttons by which the reader can vote on whether the feature would be useful or not, and the coder further invites the customer to offer a price for the project. In short,

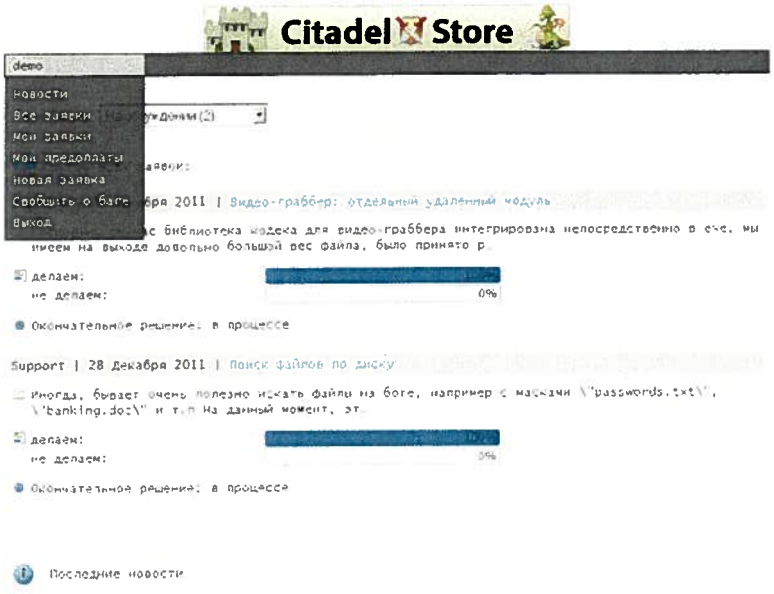
he is relying upon the customers to treat Citadel code as a common project for which they hire him when they desire new features.

84. 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. 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.

85. This screenshot shows the responses of four Citadel customers: "bigqik," "Datek," and "Kradum." Kradum's response is particularly interesting, in that he asks that the Citadel antivirus functionality be capable of "killing" "Zeus" and "SpyEye," two related financial fraud botnets that compete with Citadel using similar techniques. A fourth customer, "Sun_Stalker," appears to have entered an appearance without posting a response.

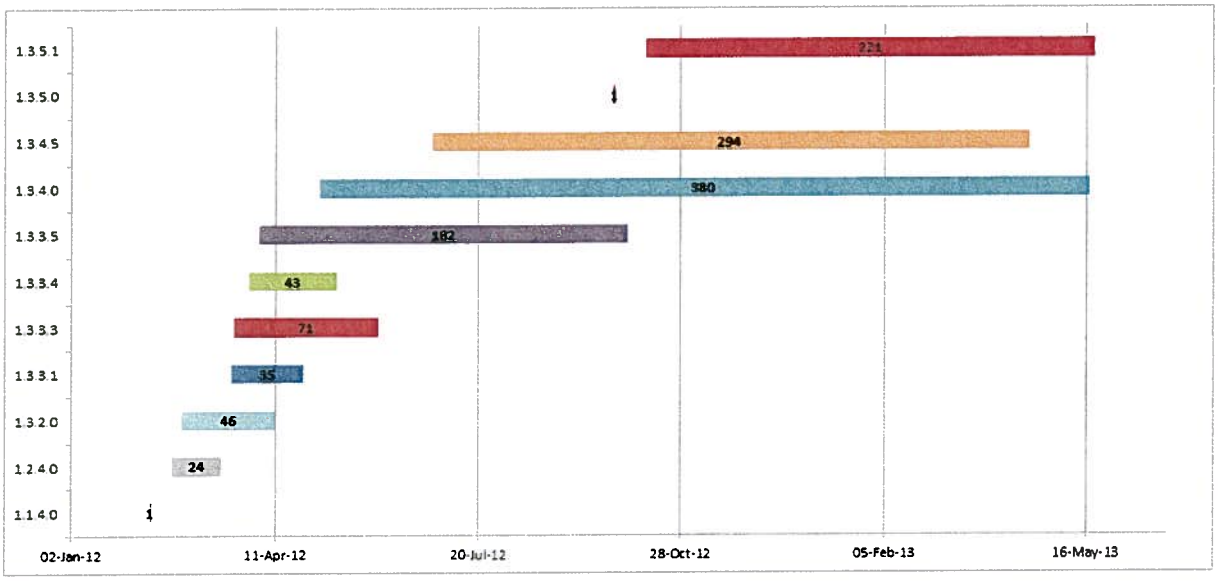
86. Although in Russian, Figure 14, below, shows a post containing a similar type of exchange between the developers of Citadel and their customers.

Fig. 14



87. The developer of Citadel 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. Figure 15, below, shows the versions of Citadel released and their lifecycle in the black market. The fast pace of updates demonstrates the intensity and the amount of work being done to improve Citadel as an implement of cybercrime and the level of cooperation between the Citadel developers and their customers. Figure 15 shows that in the first six months that Citadel has been available, the developer released five versions of the build-kit. Each release fixed bugs and added new features. Starting with version 1.3.3.5, released in April 2012, it appears that the developer had arrived at a more stable (i.e., less buggy), and more feature complete version of Citadel as evidenced by the longer duration of that version in on the Internet. Subsequent versions of Citadel have also stayed on the market for longer periods of time, consistent with a maturing cybercrime product.

Fig. 15



VI. DEFENDANTS

A. John Doe 1, Creating, Commercializing, And Supporting Citadel

88. As part of my investigation, I have studied numerous versions of Citadel bots, numerous configuration files, and I have detected and mapped the command and control infrastructures of many separate Citadel botnets. Further, I have reviewed information on the versions of Citadel available in the cybercrime black market, and information available on Citadel CRM and other cybercrime forums. Additionally, I have consulted with other investigators from private industry, academia, and the government, and I have confirmed that the evidence I have gathered and the conclusions I have reached are consistent with what other investigators have found or determined.

89. Based on this, I have determined that John Doe 1 is the developer of Citadel. He has developed and commercialized Citadel through the following acts:

a. Designing and developing the Citadel bot code and all of the modules that enable a Citadel bot to conduct theft;

b. Creating a build-kit that their customers can purchase and then use to quickly generate bots and configuration files, which are the primary means of conducting financial theft;

c. Selling the Citadel build-kits in an online Citadel store to other criminals; and

d. Providing after-sales service and support to their customers in the form of bug fixes, new features, frequently updated versions of Citadel, and a customer support interface known as Citadel CRM.

B. John Does 2-82, Creating And Operating Citadel Botnets And Conducting Criminal Acts Through Them

90. I have determined that there are 81 separate Defendants who have created and operate over 1300 Citadel botnets and who conduct criminal acts through them. I have conducted a multi-step analysis of available evidence, which I will explain in the following paragraphs.

91. First, when a Citadel customer purchases a Citadel builder-kit, they receive a product encryption key that is then built into the Citadel bot code. Over the course of my investigation, I have extracted and analyzed the product key codes used in over 52,000 Citadel bots and determined there are 101 separate Citadel keys being used. Since each Citadel product key is associated with only one Citadel Builder Kit, this indicates that there are 101 Citadel Builder Kits that have been or are being used to build, deploy, and operate Citadel botnets.

92. Botnet operators can use the same build kit to create and deploy more than one Citadel botnet. Presumably in order to differentiate between their different Citadel botnets, the botnet operators appear to give each botnet a different name. Each bot associated with a particular Citadel botnet carries that name. Therefore, from the many Citadel bots I have

analyzed, I have also extracted the names of the different Citadel botnets of which each bot in a member. I have then correlated the botnet name to the Citadel product key also extracted from the bots. The evidence shows that many of the Citadel Builder Kits have been used to build over 1300 botnets. In many cases, it appears that the botnet operator has used a common naming convention to name the different botnets, which further reinforces my conclusion that each product key is being used by one defendant to create one or more botnets. Attached as Exhibit 24 is a true and correct copy of information that I have compiled regarding the John Does. I have indicated the product keys associated with each John Doe and the various botnet names that I found associated with each product key.

93. As I discussed above, to deploy and operate a botnet, the botnet operator needs to create an infrastructure of command and control servers. These command and control servers are also listed in the configuration files that I have studied. Therefore, I have been able to associate a set of command and control servers with each Citadel botnet name.

94. Finally, I have downloaded the registration information for each domain associated with the Citadel botnets I have been investigating. As I explained above, in most investigations I have conducted, we eventually learn that most of this registration information is false or stolen. The e-mail addresses given, however, are often monitored by the botnet operators and provide a means of communicating with them. I have included some of the registration information in Exhibit 24. However, commonalities in the registration information used by the botnet operators when they set up the command and control infrastructure suggests that, at least in some cases, a single botnet operator is using multiple Citadel product keys.

95. In summary, I have determined that there are 81 John Does, each holding one or more Citadel keys, and, among them, deploying over 1300 Citadel botnets, doing business as the

names given for domain registration purposes. Each of John Does 2-82 has participated in the Citadel enterprise through the following acts:

a. Purchasing a Citadel Builder Kit and using it to generate bots and configuration files to control the bots;

b. Deploying the bots under one or more botnet names;

c. Creating a command and control infrastructure made of server computers connected to the Internet through which to communicate with the deployed bots;

d. Using one or more means to cause end-user computers to become infected with Citadel;

e. Using the Citadel bots infecting the computers of end-users around the world to steal security identification and financial account information;

f. Using Citadel bots to steal money directly from the financial accounts of unsuspecting end-users around the world;

g. Damaging Microsoft-owned and licensed software including Windows and Internet Explorer, corrupting the behavior of these programs to convert them to instruments of criminality; and

h. 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.

96. Further, evidence indicates that one or more of John Does 2-82 have conducted the following illegal activities:

a. Using Citadel bots to send illegal spam e-mail;

b. Using Citadel bots to cause secondary infections, such as by the Reveton ransomware on victim computers; and

c. Using Citadel bots to launch distributed denial of service attacks on financial and other institutions.

97. The evidence also strongly suggests that John Doe 1, who created and who has commercialized and supported Citadel, and John Does 2-82, have continuously supported a common Citadel enterprise. There is no clearer example of this than Figure 13 on page 33 of this Declaration. That Figure shows a post from John Doe 1 to his customers suggesting a new feature, and asking whether his customers want the new feature and how much they will pay him to create it. This strongly suggests that the model by which Citadel has been developed and through which it is maintained is one in which there is one coder, John Doe 1, and many users of Citadel, all of whom compensate John Doe 1 by paying him for specific improvements that he or they suggest to the code. John Does 2-82 thus appear to continually reinvest proceeds from their criminal acts in the Citadel enterprise.

98. The success of this model is strongly suggested by the history of Citadel in the cybercrime black market. This is shown in Figure 15 on page 36 of this Declaration. That shows that Citadel has been on an unusually fast release schedule, suggesting that John Does 1 and John Does 2-82 are cooperating extensively to identify bugs, prioritize new features, and to compensate John Doe 1 for fixing the bugs and developing the new features. John Doe 1 supports the criminal activities of all of the Citadel botnet operators by selling them new versions of Citadel and providing service and support such as bug fixes and manuals.

VII. TAKING DOWN CITADEL

A. A Piecemeal Approach Will Not Work

99. As discussed above, Citadel is designed to resist technical mitigation efforts,

eliminating viable technical means to curb the injury being caused and are designed to destroy evidence of and conceal the misconduct.

100. Given the specific architecture of Citadel botnets, I believe that if provided advance notice that the command and control domains and IP addresses were to be redirected to secure computers, thus disabling them, the Defendants would take measures to keep the Citadel alive by migrating the command and control infrastructure to new IP addresses and domains. As discussed above, the botnets are designed to withstand technical counter-measures:

101. Citadel has an extensive Command and Control Tier, giving each infected end-user computer multiple points of contact with the botnets. It changes the domains and IP address of the command and control servers over time. The Defendants are able to generate an alternate list of fallback rendezvous domains should the infected end-user computers be unable to communicate with the command and control servers.

102. Therefore, a piecemeal approach to disconnecting Citadel' command and control servers will fail. Unless all of the domains and IP addresses of the current command and control infrastructure are redirected to secure computers immediately and simultaneously, there is a chance that the Defendants will be able to migrate the command and control infrastructure to new servers.

103. Further, unless all of the domains and IP addresses of the command and control infrastructure are redirected to secure computers, the Defendants may be able to access those computers, thus destroying evidence of their misconduct and their identities, and destroying evidence of the infected computers that connect to the command and control servers, thus preventing mitigation and cleaning of those victim computers at a future point in time.

104. I am specifically aware of a previous instance in which the botnet controllers

changed the location of a botnet's command and control servers after services to the hosting company supporting those servers were interrupted by enforcement efforts. In that instance, the command and control server was allowed back on line for a brief interval of time, during which the command and control servers were moved to new locations in Russia and Ukraine, and the infected end-user computers were directed to the new locations.

105. I am aware of other prior instances where security experts or the United States government attempted to curb injury caused by botnets, but inadvertently allowed the bot-herders to receive notice. In these cases, the bot-herders immediately moved the botnet command and control servers to new, unidentified locations causing the botnet to continue its operations while also destroying and/or concealing evidence of the botnet's operations.

B. <u>A Coordinated Plan Is Required To Disable Citadel</u>

106. Based on my experience involving Internet security matters and disabling of botnets, I believe that the most effective way to disable Citadel is to follow the protocol set forth in the [Proposed] *Ex Parte* Temporary Restraining Order, Seizure Order and Order to Show Cause Re Preliminary Injunction ("Proposed TRO"). An explanation of the protocol in the Proposed TRO is set forth in detail in the Declaration of my colleague, David Anselmi, filed along with my own Declaration.

107. There are several goals of this protocol: 1) to halt the operation and spread, to the extent possible, of the most significant portion of the Citadel infrastructure that we have been able to identify, 2) to take control of the Citadel command and control infrastructure, 3) to remediate infection of end user computers by responding to requests those computers make to the command and control servers with content that informs users in their web browsers that their computers are infected and allows users to access antivirus and security resources that enables them to clean their computers and 4) to preserve evidence of criminal activity. .

108. It is my opinion that unless the steps described above are taken in accordance with the protocol outlined in the Declaration of David Anselmi and the Proposed Order, the injury caused by the Citadel will continue and will be compounded, and evidence of Defendants' misconduct and the botnets' operation will be moved or destroyed.

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

Executed this 28th day of May, 2013

Vishant Patel