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 PAMELA MOORE IN SUPPORT OF MICROSOFT'S APPLICATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER, SEIZURE ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

I, Pamela Moore, declare as follows:

1. I am the Senior Vice President, Administrative Services and Chief Financial Officer of NACHA-The Electronic Payments Association (NACHA). I make this declaration of my own personal knowledge and, if called as a witness, I could and would testify competently to the truth of the matters set forth herein.

2. In my role at NACHA, I have worked with forensic investigators supporting NACHA and have conducted an assessment regarding the financial and business impact of the phishing e-mails falsely purporting to be from or associated with NACHA and tied to the Citadel Botnets. The Citadel Botnets have caused, and continue to cause, extreme harm to NACHA and its members, which, if allowed to continue, will be compounded as the case proceeds.

NACHA and the ACH Network

3. NACHA is a non-profit association which manages the development, administration, and governance of the ACH Network, the backbone for the electronic movement of money and related information between financial institutions in the United States. NACHA represents more than 10,000 financial institutions via 17 regional payments associations and direct membership. In 2012, over 16.75 Billion ACH payments were processed between Financial Institutions on behalf of their customers, via an ACH Operator. As many as 145 million Americans use Direct Deposit via ACH to receive their pay or government benefits.

INJURY TO NACHA CAUSED BY THE CITADEL BOTNETS

4. Since January of 2012, under cover of emails that falsely purport to be from or associated with NACHA, the defendants have orchestrated a pernicious, growing and costly phishing scam ("Phishing Scam") that has touched or affected millions of people, and countless computers and networks around the globe.

5. I have reviewed the Declaration of Vishant Patel, which sets forth facts establishing that the emails in the Phishing Scam, which misuse NACHA's name and trademarks, are designed to infect victims' computers with malicious software referred to as the Infection Tier and to make those computers part of one or more botnets, known as the Citadel Botnets. Once infected and part of the Citadel Botnets, the defendants use the malicious software to steal the victims' account credentials and to steal funds from the victims' accounts. The Declaration of Vishant Patel also sets forth facts that the defendants in this case are responsible for the Phishing Scam and the Citadel Botnets.

6. Despite the best efforts of NACHA to mitigate the devastating effects of this phishing scam, the Phishing Scam continues to evolve in ways that cannot be sufficiently

addressed by NACHA or the Phishing Scam's victims without aggressive intervention.

A. An Overview – from Phishing Email to Botnet to Stolen Information

7. Although technical aspects of the Phishing Scam continue to rapidly and cunningly evolve, each new attack begins with an unsolicited email which falsely purports to be from NACHA, or in some way associated with NACHA, Direct Deposit or the ACH transactions for which NACHA sets standards. Recipients duped into clicking a falsified link embedded in a scam email are then connected to a series of malicious servers, the purpose of which is to download malicious software (often called "malware") onto the victim's computer. Once downloaded, that malware hijacks the victim's computer and makes it part of the Citadel Botnets. The defendants may then steal banking, payment, and other information via, for example, keystroke logging software.

8. Over time, the Phishing Scam has expertly evolved, including the methods of implementation (e.g., from offering false .doc files to drive-by-download), delivery (from php file to .jar file), obfuscation and payload (e.g., from Zeus variant, to Citadel Botnet to Blackhole rootkit). Technical aspects of the Phishing Scam are outlined in detail below.

B. Millions of Emails and Number of Attacks: An Advanced Persistent Threat

9. The Citadel Botnet is a descendant or variant of the Zeus botnet, which dates back to 2006. The first significant impact to NACHA directly due to the type of phishing attack that both Zeus and Citadel specialize in was detected in November 2009. During the timeframe of November 2009 to present the scale and nature of the attacks perpetrated by Zeus, and more recently Citadel, has varied. Although Phishing Scam emails are down from their peak in August of 2011 in which 167 million phishing emails in a single twenty-four hour period occurred, in 2012, several socially engineered e-mail phishing campaigns targeted NACHA

around normal business payment processing dates, including first of the month, end of the month and bi-monthly payroll processing dates. NACHA was one of several brands that were targeted, dependent on their primary consumer or business process activity. In 2013, two active campaigns were launched during mid February 2013 and the first week in April 2013 with average phishing emails of 3.7 million per event. A phishing e-mail campaign in early April 2013 targeted international consumers and businesses, informing them of upcoming changes to US based International ACH Transactions (IAT). Attached is Exhibit 1, a true and correct copy of a phishing email falsely purporting to be from NACHA, utilizing NACHA logo and trademarks, all hyperlinks contained within the phishing e-mail pointed to a compromised website. By contrast to this enormous volume of Phishing Scam emails, NACHA's normal volume for authentic outbound e-mail messages is only 1,000 emails per day.

10. NACHA is able to estimate and track the scale of the attack phase of the Phishing Scam because, naturally, it is the mail exchange (MX) authority for the "nacha.org" domain. As a result, all spam for that domain gets bounced back to NACHA's servers, including emails that spoof nacha.org emails. In addition, NACHA uses various other sources and metrics to estimate the number of phishing emails, including security policies and reports from security vendors and vendors helping to eliminate spam.

11. For example, in the week from April 2, 2013, through April 9, 2013, over 3.7 million phishing emails, purporting to be from the "nacha.org" domain name, were sent from over 64,000 servers. In fact, there are only a handful of authentic NACHA servers for e-mails, illustrating the scale of the fraud. Attached as Exhibit 2 is a true and correct copy of a report by Agari Data, Inc., formerly known as Authentication Metrics, Inc., demonstrating these facts. Notably, because the report only tracks emails purporting to be from "nacha.org," and not from

any of the many other domain names used by the defendants to trick Phishing Scam victims, such as "nachas.org," such reports necessarily underestimate the actual number of Phishing Scam emails.

12. NACHA maintains an e-mail address in which consumers and businesses can forward potential spam e-mails at abuse@nacha.org. These reported e-mails are used for analysis of attacks against NACHA and for forensics and for reporting malicious URLs, in the hope of receiving voluntary assistance by domain registries and registrars. However, these voluntary efforts are not sufficient to disrupt the attacks, as informal assistance regarding malicious URLs are piecemeal and cannot be coordinated across the entirety of the malicious infrastructure. Attached as Exhibit 3 is a true and correct copy of email subject lines forwarded to abuse@nacha.org from January 2013 to May 2013. The prolonged and sustained attack on Direct Deposit and ACH transactions has damaged the reputation of NACHA and the ACH Network. Individuals receiving these spam e-mails may now have become hesitant to utilize ACH payment transactions or online banking and bill payment services in the future. It is negatively impacting not only NACHA and the ACH Network, but potentially all financial institutions that help support their consumers and businesses who utilize Direct Deposit and Direct Payment via ACH. The scale of the Phishing Scam attacks is beyond the ability of NACHA to deal with alone. The assistance of the Court is desperately needed to dismantle large portions of the infrastructure in a coordinated manner.

13. NACHA utilizes a security vendor for purposes of analysis of suspicious URLs either sending phishing e-mails or within hyperlinks contained in the phishing e-mails. Since January 2012, NACHA has initiated 194 malware takedowns. Attached is Exhibit 4, a true and correct copy of the malware delivery URLS taken down.

14. NACHA is extremely concerned that the notoriety of the Phishing Scam has inspired other criminals to engage in copycat or similar tactics to obtain consumer information, hence further complicating NACHA's battle against the existing perpetrators. The Citadel malware is a Zeus malware variant used to relay not only password data, but other basic information about a victim's PC that can then allow for potential exploits based on the version of the victim's computer operating system or default browser, as well as providing shared network information. In 2012, after a prolonged Phishing Scam attack in 2011, the Citadel malware was identified as "an "open source" version of the Zeus Trojan whose defining feature is a social networking platform where users can report and fix programming bugs, suggest and vote on new features, and generally guide future development of the botnet malware". Attached is Exhibit 5, a true and correct copy of an article written February 9, 2012 on the "Krebs on Security" website discussing the rapid growth of the Citadel Trojan. In November of 2012, the FBI released a public notice alert regarding updated activity related to the Citadel malware. Attached is Exhibit 6, a true and correct copy of the FBI news release.

C. Public Interest Concerns

15. In addition to the costs to NACHA, there is likely an immense number of computers, companies and individuals worldwide that have been affected by the Phishing Scam and the Citadel Botnets into which victims are unknowingly trapped. One may reasonably assume that the Citadel Botnets spread through the Phishing Scam may be used to obtain affected computer user information, which of course includes financial and personal information that can be exploited in such a way as to cause millions upon millions of dollars in direct losses. Thus, NACHA believes it is extremely important and urgent to address this particular attack.

16. The Phishing Scam is sophisticated and, as result, it is clear that the defendants

will continue to exploit it as long as it is goes unchecked. Although NACHA has taken measures to address the Phishing Scam expeditiously and in the best way it knows how, the sophistication of the attacks and NACHA's limited ability to identify the sources of the attack will continue to make it very difficult to stop these attacks from continuing to increase at an alarming rate.

17. Moreover, it is important to consider the disadvantage NACHA has in that it does not have relationships with the intended victims of the Phishing Scam, unlike in the case of a similar attack on the customers of a financial institution, such as XYZ Bank. If the defendants were to target the customers of XYZ Bank, XYZ Bank would be in a position to send informative notices of the fraud directly to its customers, both by email and regular mail, either as separate notices or as part of a pre-scheduled delivery, such as the delivery of an account statement. In contrast, because NACHA does not have any relationship with the intended victims of the Phishing Scam, NACHA does not have an existing, verifiable way to communicate with those victims.

D. Overview of Recent Attacks

18. Although the Phishing Scam has evolved over time, it has always entailed multiple layers which serve to hide the identity and source of the attack.

a. **Phishing Email.** The initial mode of attack was a falsified e-mail with spoofed header information and content. Those emails were distributed through open relays, which allowed the attackers to hide the IP addresses of the compromised or malicious servers. The e-mails would falsely claim to be from NACHA, but would invariably include text masquerading as an error message from or in connection with NACHA or an ACH transaction. The false message invited the recipient to read a report of the error that could be accessed, according to the e-mail, through a link to a URL where the report could be found. The link made

it look like the user would be opening a .pdf file because it showed the end of the url as ".pdf". In reality, however, the link ultimately led – through a series of proxy computers - to an executable file having a filename of the form <something>.pdf.exe.

b. **Current Forms of Attack.** At this time the following two forms of attack have been observed, both consistent with the type of attack conducted by the Zeus botnet, and its offspring, Citadel. The first method is a three layer attack. The first layer is a compromised web server with the index.html redirector. In each index.html file there are three to five links to JavaScript redirectors that make up the second layer of the attack. The entry point URLS are embedded in the emails that are forged to seem to come from NACHA. An entry point URL has the following format: hxxp://www.summersoftlabs.com/gPJcnezm/index.html. The format of the email changes for each wave of the attack, but consistently leverages NACHA's brands in one way or another. Currently all landing page URLS are connected to centralized secondary location. This centralized place is where the binaries are using the Blackhole rootkit are being served. Beginning in early September 2012 this centralized location was down for a significant period of time. During these periods the system that creates hosting at Virtual Private Servers to host the landing pages was still functioning, as was the system that creates the entry point URLS and javascript redirectors. The spam generation system was also still fully functional and sending out waves of the attack during these periods. During 2012, nearly 600 unique javascript redirector URLs were identified during NACHA's investigation on the Phishing Scam, and very little activity from this method has been seen in 2013.

c. The other form of attack that is being used is the simple two-layer attack with an entry point URL in the spam with a format like the following:

hxxp://tilatequilablog.com/wp-content.htm

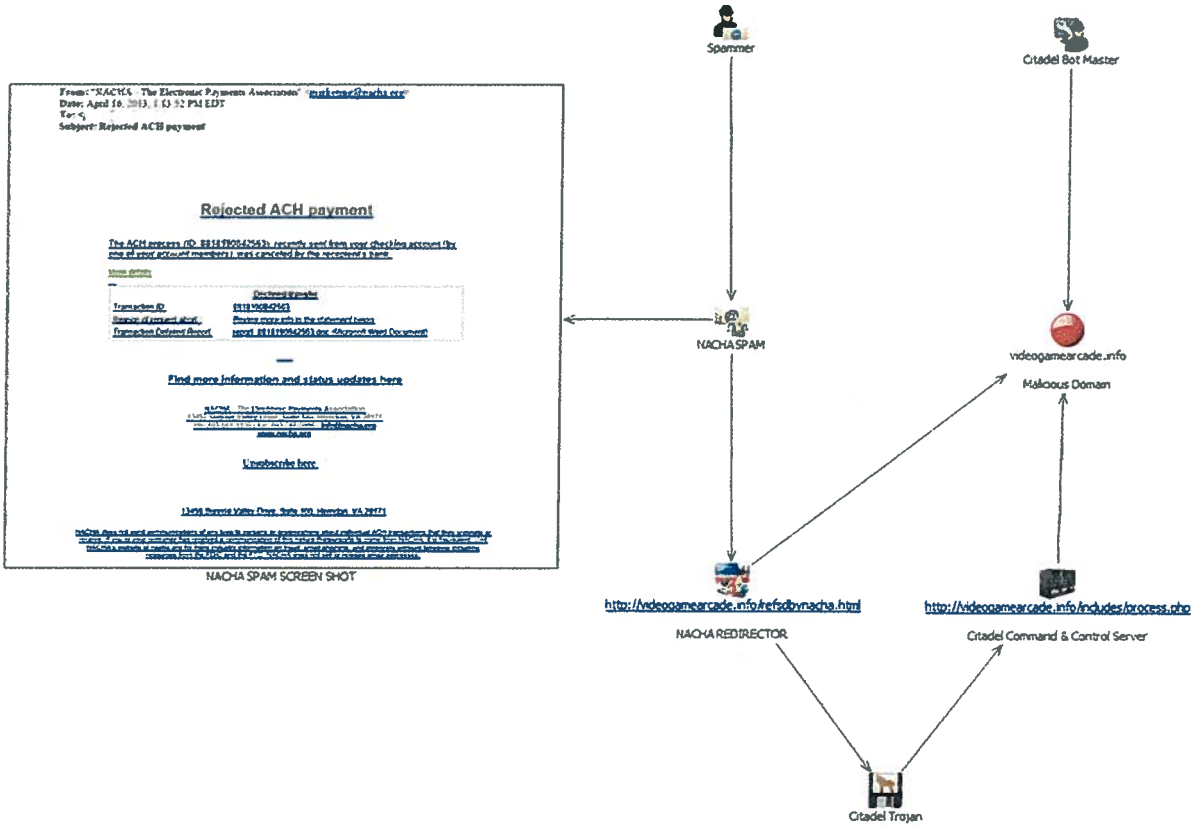
As can be seen, this URL follows a different format than the entry point URL of the three layer attack, described above. Such URLs are spread by similar types of spam as the three-layer attack. The difference is that each set of these URLs redirects the victim to the same landing page. There is no variation in landing pages within each wave of this attack. These landing pages utilize the Blackhole rootkit and pull binaries from the same centralized location as the three-layer attack. This is confirmed by the fact that they exhibit the same downtime periods as the three layer landing pages. Even though this second form of the attack is only incorporating one single landing page per wave, these landing pages are protected by fairly complex countermeasures. First, they use a single domain name, but the DNS for the domain name points to multiple IP addresses and the pool of these addresses can be replenished as the existing ones are taken down. Second, the DNS servers for landing pages that run the round-robin DNS are actually rogue servers controlled by the attackers. These rogue servers are registered under the fraudulent domain names that are also registered by the attackers. Since they run these rogue servers in pairs with a primary and a backup, it is difficult to get both of them taken down before a third is added to the set of DNS servers for the landing page domain.

19. In the later versions of the attack, the servers with the malware appear to be hosted exclusively on malicious VPS platforms that were purchased for the express purpose of serving malware. The attackers have knowledge of the fraud prevention systems for many VPS providers and have been able to actively game that system by producing anywhere from 3 up to 10 new VPS accounts per day. Since the hosting provider and the registrar are different organizations, the attackers can adapt to informal take down attempts. When a reported VPS target is taken down after the host was placed on notice of the Phishing Scam, it takes some time before the actual domain is taken down because the appropriate registrar has to be found and

notified. The defendants continue to have access to the management interface for the domain and are able to point the DNS for the domain to a new VPS. As a result, this approach behaves essentially like a fast flux attack and makes it more difficult to address from the NACHA's perspective.

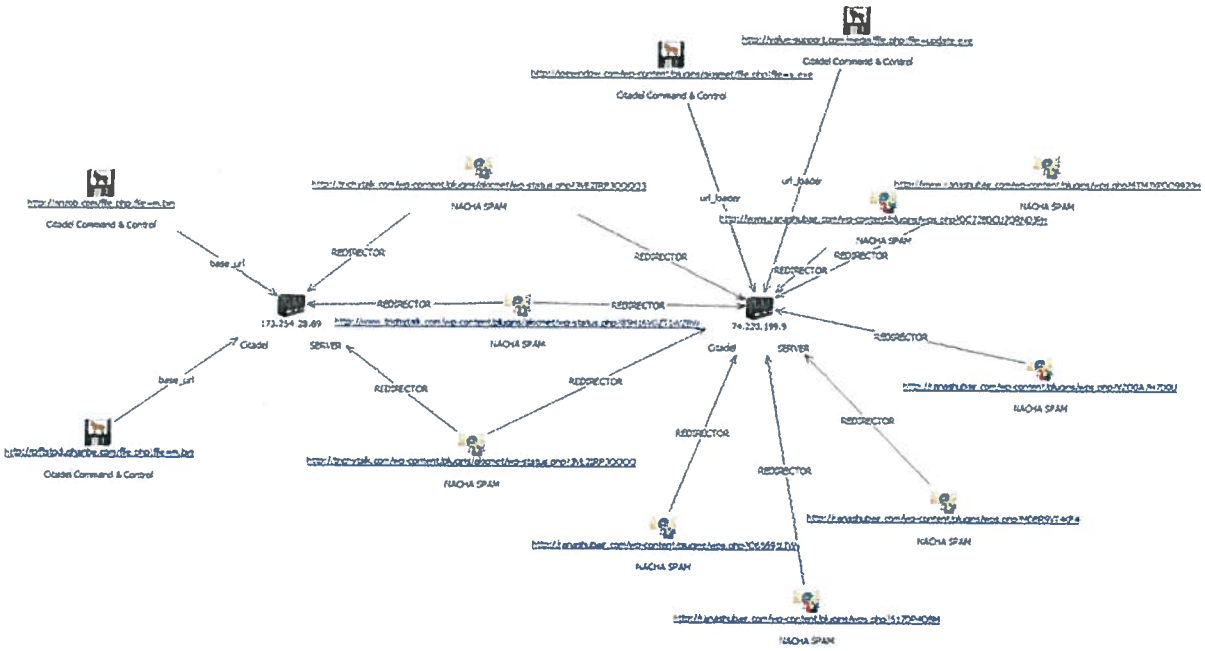
20. During 2012 to present, over 16,900 redirector URLs were identified as part of NACHA's investigations on the Phishing Scam, some of which were compromised webpages of legitimate websites. Figure 1, below, provides a graphic representation of the Phishing Scam.

Fig. 1



21. Attached in Exhibit 7 is a true and correct copy of over 1690 redirector URLs directly tied to the Citadel Botnet. Figure 2, below, provides a graphic representation of the Citadel Botnet:

Fig. 2



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

Pamela Moore

Pamela Moore