

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 ERIC GUERRINO

I, Eric Guerrino, declare as follows:

1. I am Executive Vice President of the Financial Services Information Sharing & Analysis Center (FS-ISAC). 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.

FS-ISAC

2. The FS-ISAC was formed in 1999 in response to the 1998 Presidential Decision Directive 63 (PDD63) that called for the public and private sector to work together to address cyber threats to the Nation's critical infrastructures. After 9/11, and in response Homeland Security Presidential Directive 7 (HSPD7) and the Homeland Security Act, the FS-ISAC expanded its role to encompass physical threats to our sector.

3. The FS-ISAC is a 501(c)6 nonprofit organization and is funded entirely by its

member firms and sponsors. In 2004, there were only 68 members of the FS-ISAC, mostly larger financial services firms. Since that time the membership has expanded to over 4,400 organizations including commercial banks and credit unions of all sizes, brokerage firms, insurance companies, payments processors, and over 20 trade associations representing the majority of the U.S. financial services sector.

4. The FS-ISAC works closely with various government agencies including the U.S. Department of Treasury, Department of Homeland Security (DHS), Federal Reserve, Federal Financial Institutions Examination Council (FFIEC) regulatory agencies, United States Secret Service, Federal Bureau of Investigation (FBI), National Security Agency (NSA), Central Intelligence Agency (CIA), and state and local governments, as well as U.S. CERT.

5. With respect to cooperation within the financial services sector, the FS-ISAC is a member of, and partner to the Financial Services Sector Coordinating Council (FSSCC) for Homeland Security and Critical Infrastructure Protection established under HSPD7 and its successor, PPD 21. We also work closely with other industry groups and trade associations that are members of the FS-ISAC including the American Bankers Association (ABA), Securities Industry and Financial Markets Association (SIFMA), Independent Community Bankers Association (ICBA), and the BITS division of the Financial Services Roundtable. In addition, our membership includes various payments, clearing houses and exchanges such as the National Automated Clearing House Association (NACHA), Depository Trust and Clearing Corporation (DTCC), New York Stock Exchange, NASDAQ, The Clearing House (TCH), the various payment card brands and most of the card payment processors in the U.S.

6. The overall objective of the FS-ISAC is to protect the financial services sector against cyber and physical threats and risk. It acts as a trusted third party that allows members to

submit threat, vulnerability and incident information in a non-attributable and trusted manner so information that would normally not be shared is able to be provided from the originator and shared for the good of the sector, the membership, and the nation. The FS-ISAC represents the interests of its financial services industry members in combating and defending against cyber threats that pose risk and loss to the industry. Among other activities carried out on behalf of its members, FS-ISAC develops risk mitigation best practices, threat viewpoints and toolkits; provides technical, business and operational impact assessments; recommends mitigation and remediation strategies and tactics; and facilitates member sharing of threat, vulnerability and incident information.

Injury To FS-ISAC Members Caused By The Citadel Botnets

7. I have conducted an assessment regarding the impact of financial account takeovers carried out through botnets on the financial institution members of FS-ISAC, on the financial services industry generally and on consumers who carry out financial transactions online.

8. Through my role and experience at FS-ISAC, I have knowledge relating to reporting of online banking fraud by FS-ISAC members to various government agencies such as (1) The Federal Deposit Insurance Corporation (“FDIC”), the agency that identifies, monitors and addresses risks to deposit insurance funds; and (2) FinCEN, a bureau of the U.S. Department of the Treasury with a mission of enhancing U.S. national security, deterring and detecting criminal activity, and safeguarding financial systems from abuse.

9. The FDIC and FinCEN receive a variety of confidential reports from financial institutions regarding online banking fraud. A majority of the incidents reported to the FDIC and FinCEN relate to malicious software on online banking customers’ computers. Typically, a

victim is tricked into visiting a malicious website or downloading malicious software that gives perpetrators access to victims' banking passwords and credentials. The perpetrators use that information to transfer money out of victims' accounts using the Automated Clearing House (ACH) system or the Federal Reserve's Fedwire transfer system. Both the ACH and Fedwire systems are used by banks and credit unions to process payments on behalf of their customers.

10. Since 2005, financial institutions have reported to FDIC and FinCEN a cumulative \$543 million in consumer loss from such online banking fraud. The rate of such loss has been substantial in recent years and was virtually nonexistent before 2005.

11. I have reviewed the technical analysis and investigation of the Citadel Botnets, set forth in the Declaration of Vishant Patel, submitted in this case. The Citadel Botnets are used to carry out precisely the type of online banking fraud that has resulted in \$543 million in consumer loss since 2005.

12. Mr. Patel's declaration sets forth a number of institutions targeted by the Citadel Botnets, including numerous U.S. financial institutions and NACHA, the organization that manages the ACH Network (the primary infrastructure for electronic transfers of money). Nearly all of those U.S. financial institutions and NACHA itself are members of FS-ISAC and FS-ISAC represents their interests in protecting these financial institutions, consumers and the industry from cybercrime and fraud.

13. I have independently discussed the Citadel Botnets with financial institution members of FS-ISAC and with NACHA, which have collected and analyzed information regarding the Citadel Botnets. FS-ISAC's members report that they view the Citadel Botnets as a major threat, which damages their brands and causes injury to both consumers engaged in online banking and the financial services industry generally.

14. Based on the analysis set forth in Mr. Patel's declaration, information provided to me by FS-ISAC's members, and my knowledge of the impact of such activities on FS-ISAC's members, I conclude that the Citadel Botnets have caused, and continue to cause, extreme damage to FS-ISAC members, consumers and the financial industry. If allowed to continue, such damage will be compounded as this case proceeds.

15. While the Citadel malware is relatively new, at least one third party report indicates that, if left unchecked, the Citadel Botnets could grow to become a very significant part of the overall online banking fraud loss reported each year by FS-ISAC's financial institution members and by NACHA. Specifically, in May 2010, the technology company Unisys issued a report entitled "Zeus Malware: Threat Banking Industry," which estimated that the Zeus Botnets, of which the Citadel Botnets are a variant, had targeted more than 960 different banks and had stolen over \$100 million since its inception in approximately 2007. A true and correct copy of the Unisys report is attached to this declaration as Exhibit 1.

16. Based on the analysis set forth in Mr. Patel's declaration, information provided to me by FS-ISAC's members and my knowledge of the impact of such activities on FS-ISAC's members, I conclude that the defendant operators of the Citadel Botnets access without authorization information from financial institution servers. I conclude that through such intrusion, defendants steal account credentials and other personal information from the customers of those FS-ISAC members and ultimately steal money from the accounts of those customers. I have also confirmed with FS-ISAC members that they have collected and observed evidence of such access without authorization from financial institution servers, in order to steal information and funds. This activity causes injury to the FS-ISAC member institutions and their customers.

17. Based on the analysis set forth in Mr. Patel's declaration, information provided to

me by FS-ISAC's members and my knowledge of the impact of such activities on FS-ISAC's members, I conclude that the defendant operators of the Citadel Botnets make counterfeit copies of the trademarks of financial institutions that are FS-ISAC members, including but not limited to the trade names of such financial institutions, the trade name of NACHA, and the trademark logos of these institutions. I have also confirmed with FS-ISAC members that they have collected and observed such evidence of trademark infringement carried out by the Citadel Botnets. I further conclude that defendant operators of the Citadel Botnets use those counterfeit trademarks in spam email or on fake web pages, in order to deceive consumers and to carry out schemes enabling the theft of personal information and funds from the financial institutions and their customers. This activity causes injury to the FS-ISAC member institutions, by diminishing their brands and goodwill. This activity causes injury to the FS-ISAC member institutions and their customers by causing confusion to consumers and victims of such schemes, by leading them to believe that the spam email and web pages containing the counterfeit trademarks originate from the legitimate brand owner when, in fact, they do not.


18. The interests that FS-ISAC seeks to protect in this case and the injury that it is attempting to remedy, as described above, are directly related to the purposes of FS-ISAC. It is FS-ISAC's role to protect its financial institution members from cybercrime and to mitigate the threat and injury flowing from such abuse. This role is demonstrated in FS-ISAC's stated purpose and the original government mandate that led to its creation.

19. The injury described above has already occurred and continues to be immediate and threatened. This injury is common across all of FS-ISAC's members that are targeted by the Citadel Botnets and the injury, and relief sought to disable the Citadel Botnets, are not specific to any particular FS-ISAC member.

20. I conclude based on the foregoing that, unless the Citadel Botnets are disabled, the harm described above will continue and, given its scale, will irreparably damage FS-ISAC's member institutions and the financial services industry generally.

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



Eric Guerrino