

FILED

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

2015 FEB 20 A 9 22

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

MICROSOFT CORPORATION, a
Washington corporation, and FS-ISAC, INC.,
a Delaware corporation,

Plaintiffs,

v.

JOHN DOES 1-3, CONTROLLING A
COMPUTER BOTNET THEREBY
INJURING PLAINTIFFS, AND THEIR
CUSTOMERS AND MEMBERS,

Defendants.

Civil Action No: 1:15 cv 240 LMB/10D

FILED UNDER SEAL PURSUANT TO
LOCAL CIVIL RULE 5

**DECLARATION OF ERIC GUERRINO IN SUPPORT OF PLAINTIFFS’
APPLICATION FOR AN EMERGENCY EX PARTE TEMPORARY RESTRAINING
ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

I, Eric Guerrino, declare as follows:

1. I am Executive Vice President of FS-ISAC, Inc., 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 infrastructure. After 9/11, and in response to 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 5,200 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 and foreign financial institutions as well. More than 100 members are headquartered overseas in 21 different countries.

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), and other federal, state and local government agencies, 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 payment associations, 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. We have payment processors from Canada, the United Kingdom, and Singapore as members as well.

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 Ramnit Botnet

7. I have conducted an assessment regarding the impact of financial thefts 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 significant proportion 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. A July 2014 publication by Aite Group estimates losses from corporate account takeovers (banking Trojans) worldwide totaling 627 million USD.

11. I have reviewed the technical analysis and investigation of the Ramnit botnet, set forth in the Declarations of Jason Lyons, Selvaraj Karthik, Tim Liu, and Vikram Thakur (the "Co-Declarants"), submitted in this case. Based on their analysis, I am informed and believe that the Ramnit botnet carries out the type of online banking fraud that has resulted in hundreds of millions in consumer losses. For example, one FS-ISAC member observed over 30 cases of financial fraud associated with the Ramnit botnet during the time period from the beginning of March 2014 through the end of April 2014. The average net loss associated with each of these cases was over \$4,300.

12. The declarations of the Co-Declarants set forth a number of institutions targeted by the Ramnit botnet, including numerous financial institutions that are members of FS-ISAC. FS-ISAC represents its members' interests in protecting financial institutions, consumers and the industry from cybercrime and fraud.

13. I have independently discussed the Ramnit botnet with financial institution members of FS-ISAC, which have collected and analyzed information regarding the Ramnit botnet. FS-ISAC's members report that they view the Ramnit botnet as a continuing 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 the declarations of the Co-Declarants, 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 Ramnit botnet has caused and will continue to cause substantial damage to FS-ISAC members, consumers and the financial industry. If allowed to continue, such damage will be compounded as this case proceeds.

15. Based on the analysis set forth in the Declarations of the Co-Declarants, 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 Ramnit botnet misappropriate online banking login credentials from FS-ISAC members' customers. I conclude that through such intrusion, defendants 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 thefts. This activity causes injury to the FS-ISAC member institutions and their customers.

16. Based on the analysis set forth in the declarations of the Co-Declarants, 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 Ramnit botnet make and use 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 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 Ramnit botnets. I further conclude that defendant operators of the Ramnit botnets use those counterfeit trademarks to deceive consumers and to carry out schemes enabling the theft of online banking credentials. 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

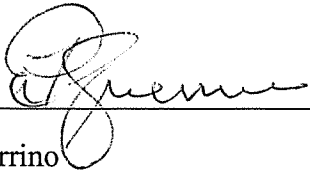
causing confusion to consumers and victims of such schemes by leading them to believe that the counterfeit trademarks and webpages created by the Ramnit botnet originate from the legitimate brand owner when, in fact, Ramnit alters them in a way that facilitates account fraud.

17. 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.

18. 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 Ramnit botnet and the injury and relief sought to disable the Ramnit botnet are not specific to any particular FS-ISAC member.

19. I conclude based on the foregoing that, unless the Ramnit botnet is 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 February 19, 2015, in Washington, D.C.



Eric Guerrino

OHSUSA:761040902.2