

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

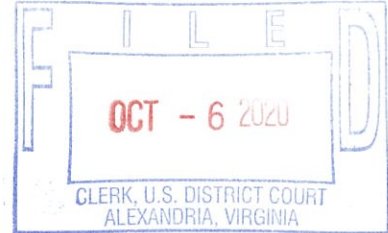
MICROSOFT CORPORATION, a
Washington corporation, and FS-ISAC, INC.,
a Delaware corporation,

Plaintiffs,

v.

JOHN DOES 1-2, CONTROLLING A
COMPUTER BOTNET AND THEREBY
INJURING PLAINTIFFS, AND THEIR
CUSTOMERS AND MEMBERS,

Defendants.



Civil Action No: 1:20-cv-1171

FILED UNDER SEAL

**DECLARATION OF STEVEN SILBERSTEIN IN SUPPORT OF PLAINTIFFS'
APPLICATION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING
ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

I, **Steven Silberstein**, declare as follows:

1. I am Chief Executive Officer of FS-ISAC, Inc., the Financial Services Information Sharing & Analysis Center ("FS-ISAC"). I make this declaration in support of Plaintiffs' Application For An Emergency Temporary Restraining 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 to the truth of the matters set forth herein.

FS-ISAC

2. FS-ISAC is a global intelligence sharing community solely focused on financial services connecting nearly 7,000 financial institutions. The organization is dedicated to helping ensure the resilience and continuity of the global financial services infrastructure and individual

firms against acts that could significantly impact the sector's ability to provide services critical to the orderly function of the global economy.

3. FS-ISAC is a 501(c)(6) nonprofit organization and is funded entirely by its member firms and sponsors. It is headquartered in the United States with offices in the United Kingdom and Singapore. Member organizations include commercial banks and credit unions of all sizes, brokerage firms, insurance companies, payments processors, and trade associations.

4. In the United States, FS-ISAC is an established industry organization with a key role in the Financial Services Sector Coordinating Council (FSSCC) and many industry-related cyber exercises. In the US alone, FS-ISAC covers approximately 5,000 financial institutions, including Section 9 critical infrastructure banks and financial market infrastructure. The FS-ISAC Cyber Threat Level is used throughout the industry to understand the current threat landscape against the sector.

5. 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. FS-ISAC members submit threat-related information for sharing amongst the membership in a non-attributable and trusted manner. This establishes a mutual defense approach to cyber risk by allowing the sector to learn from the security and fraud events and incidents of their peers. This aids in protecting the member firm and its customers. Through FS-ISAC's communities of interest and sharing channels, it builds a platform for financial institutions to share threat information, crowdsource mitigation and detection strategies, share knowledge and advice, and discuss issues at large. FS-ISAC operates an exercising program and an intelligence analysis team to assist in the building of operational resilience and the creation of strategic intelligence reports respectively.

Banking Trojans and Phishing Campaigns Designed to Steal Money From FS-ISAC Members and the Public

6. Through my role and experience at FS-ISAC, I have knowledge relating of phishing campaigns and online banking fraud reported by FS-ISAC financial institution members. Typically, a victim is tricked into visiting a malicious website or downloading malicious software via a phishing email or other means of delivery. Once a victim's device is infected with the malware, the Defendants access the victims' banking passwords and credentials. The Defendants then 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.

7. Financial malware and phishing campaigns cause significant financial harm to FS-ISAC members and the public. For example, the FBI's Internet Crime Complaint Center (IC3) produced an Internet Crimes Report that identified during 2019 over 16,000 financial malware victims causing over \$160 million in losses. Phishing attacks claimed an additional 115,000 victims in 2019 leading to almost a \$60 million loss. The American Bankers Association (ABA) 2019 Deposit Account Fraud Survey reported \$265 million worth of losses to electronic banking transactions.

8. Banking trojans are a type of malware that facilitates this type of fraud to occur. Trickbot is one such banking trojan. Trickbot is spread through phishing emails designed to mimic a trusted sender (and FS-ISAC member organizations) and steal a victim's bank account data and personally identifiable information (PII) to then commit identity fraud and steal money from the victim.

Injury To FS-ISAC Members Caused By The Trickbot Botnet

9. I have reviewed the technical analysis and investigation of the Trickbot botnet, set forth in the Declarations of Jason Lyons, Rodelio Fiñones, Vikram Thakur and Jean-Ian Boutin (the "Co-Declarants"), submitted in this case. Based on their analysis, I am informed and believe

that the Trickbot botnet carries out the type of online banking fraud that has resulted in hundreds of millions in consumer losses.

10. I have conducted an assessment regarding the impact of financial thefts carried out through Trickbot botnet on the financial institution members of FS-ISAC, on the financial services industry generally and on consumers who carry out financial transactions online.

11. Trickbot is a prolific botnet that attacks victims with multiple forms of malware, including banking trojans and phishing campaigns. Trickbot is designed to impersonate FS-ISAC members in order to perpetuate Defendants' fraud. In fact, during approximately year and a half period FS-ISAC members attributed Trickbot to over 500 fraud attempts against customer accounts, amounting to over \$7 million in attempted fraud. For example, one FS-ISAC member observed dozens of cases of attempted financial fraud associated with the Trickbot botnet over the course of two weeks. The average amount Trickbot attempted to steal in each of these was over \$268,000. Another FS-ISAC member identified Trickbot as infiltrating roughly 30 customer accounts.

12. Trickbot-related phishing campaigns also target FS-ISAC members directly. Several FS-ISAC members report thousands of Trickbot-related phishing campaigns on a monthly basis. For example, several FS-ISAC members reported the following level of attacks in September:

- a. One FS-ISAC member reported hundreds of phishing attacks within a four-day period between September 1-4, 2020;
- b. One FS-ISAC member reported 1,720 phishing attacks in September;
- c. One FS-ISAC member reported 1,445 phishing attacks in September, representing an increase in frequency by the hundreds over the previous month;
- d. One FS-ISAC member reported 1,178 phishing attacks in September;
- e. One FS-ISAC member reported 1,125 phishing attacks in September; and
- f. One FS-ISAC member reported over 600 phishing attacks in September.

13. Two additional members reported 2075 and 614 phishing and/or malware infections, respectively, from another malware, Emotet, which is known to distribute and disseminate Trickbot.

14. My staff and I have independently discussed the Trickbot botnet with the financial institution members of FS-ISAC, which have collected and analyzed information regarding the Trickbot botnet. FS-ISAC's members report that they view the Trickbot botnet as a continuing threat, which damages their brands and causes injury to both consumers engaged in online banking and the financial services industry as a whole.

15. Based on the analysis set forth in the declarations of the Co-Declarants, information provided to me by FS-ISAC members, and my knowledge of the impact of such activities on FS-ISAC's members, I conclude that the Trickbot botnet has caused and will continue to cause material damage to FS-ISAC members, consumers and the financial industry. If allowed to continue, such damage will be compounded as this case proceeds.

16. Based on the analysis set forth in the Declarations of the Co-Declarants, information provided to me by FS-ISAC members and my knowledge of the impact of such activities on FS-ISAC's members, I conclude that the defendant operators of the Trickbot 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 FS-ISAC member institutions and their customers.

17. 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 Trickbot 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 Trickbot botnets. I further conclude that defendant operators of the Trickbot 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 Trickbot botnet originate from the legitimate brand owner when, in fact, Trickbot alters them in a way that facilitates account fraud.

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

20. I conclude based on the foregoing that, unless the Trickbot 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 October 4, 2020, in Alexandria, Virginia.



Steven Silberstein