EXHIBIT 1

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

DECLARATION OF DAVID ANSELMI IN SUPPORT OF PLAINTIFFS' MOTION FOR DEFAULT JUDGMENT AND PERMANENT INJUNCTION

1. I am a Principal Investigator in the Digital Crimes Unit of Microsoft Corporation's Legal and Corporate Affairs Group. I make this declaration in support of Plaintiffs' Motion for Default Judgment and Permanent 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.

2. In my current role at Microsoft, I assess technical security threats to Microsoft and the impact of such threats on Microsoft's business and customers. Prior to my current role, I worked as Senior Technologist, dealing with security of Microsoft's online services. Among my responsibilities were protecting Microsoft's customer-facing online service assets from network-based attacks. Prior to that, while also employed by Microsoft, I worked as a Senior Technologist, dealing with protecting Microsoft's corporate resources from network-based attacks. Before joining Microsoft, I worked for Excell Data Corporation as a Program Manager performing

security firewall deployment, configuration, and administration. I am a graduate of the United States Military Academy, West Point, and served for 27 years as a United States Army Communications Electronics Officer (11 years active, 16 years reserve), attaining the rank of Lieutenant Colonel. I have been employed by Microsoft since February 1997.

3. On October 6, 2020, the Court granted Plaintiffs' TRO Application. Based on the Court's Temporary Restraining Order, Plaintiffs were able to cut off communications between computers and networks compromised by the Defendants and certain IP addresses used by Defendants as a command and control infrastructure. Thereafter, the Court granted a Preliminary Injunction order.

4. Microsoft's ongoing investigation into Trickbot shows that the TRO was effective in protecting many victims targeted by Trickbot. For example, since the execution of the TRO, Microsoft interrupted roughly 80 million attempted internet connections by Defendants targeting hundreds of thousands of victims.

A. Defendants Continue To Register And Use New IP Addresses Which Are Used For Malicious Purposes And Cause Irreparable Harm To Plaintiffs And Their Customers

5. Defendants' use of IP addresses as a command and control infrastructure to further their illegal acts is described generally in the Declarations of Jason Lyons and Rodelio G. Finones filed on October 6, 2020 (Docket Nos. 15-16). I worked with Mr. Lyons and have carried out the investigation and analysis of the Trickbot botnet. Based on my participation in this work and based upon my personal knowledge of the work carried out with Mr. Lyons and Mr. Finones, I adopt and incorporate that general testimony regarding the Trickbot actors and infrastructure by reference. Defendants continue to attempt to recover from the loss of their command and control IP addresses by registering and activating the new IP addresses for use in Trickbot's command and control infrastructure. The evidence gathered further indicates that Defendants have used and are regularly

registering new IP addresses to launch new attacks on victim computers using various means.

6. I have analyzed the technical aspects of the newly registered IP addresses. In particular, I have observed the operation of the Trickbot malware, as Defendants have attempted to update the malware over the last several months. I have done so through the same system that was used previously in this matter, by which computers are intentionally infected with the Trickbot malware and communications between new versions of the Trickbot malware and the Internet are observed. This enables identification of the command and control the IP addresses that the Defendants are using to attempt to control computers infected with the malware. Through the IP addresses, we have seen Defendants send to infected end user computers the most fundamental instructions, modules, updates, and commands, and carry out overall control of the botnet. These modules, updates, and commands leverage Microsoft copyrights and trademarks as discussed more thoroughly in Mr. Finones declaration. *See generally* Dkt. No. 16. Defendants have recently used the IP addresses to download instructions or additional malware to the infected computers, carry out attacks against those computers, including installation of ransomware and theft of financial credentials.

7. Defendants have used and can continue registering new IP addresses to carry out activities prohibited by the Preliminary Injunction. In particular, the commands and information sent from and to newly registered IP addresses is used by Defendants to intentionally access and send malicious software to protected computers running the Windows operating system, in order to infect those computers and make them part of the Trickbot botnet. Through my investigation, I have concluded that the IP addresses registered since the Court's order on the Preliminary Injunction have been used to send malicious code to configure, deploy and operate the Trickbot botnet. Since the preliminary injunction, the IP addresses have been used to compromise the

computers and networks of Plaintiffs and their customers and associated member organization, including by corrupting Microsoft's operating system and applications on victims' computers and networks, by delivery malicious ransomware and by delivering malicious software designed to steal information and financial account credentials. The use of the IP address above for these purposes violates the prohibitions set forth at pages 7 and 8 of the Preliminary Injunction. (Docket No. 38)

8. Defendants continue to register new IP addresses since the Preliminary Injunction order in order to install malware on victims' Windows operating systems and install processes in Windows and Microsoft branded file paths and registry paths, in order to deceive victims and steal sensitive information from their computers. Thus, in addition to the injury caused by the malware and the botnet itself, the Defendants' practice of registering new IP addresses and the activities carried out through the IP addresses are false, deceptive, likely to create confusion among victims, and likely to create the impression that Defendants' activities or malware that they install are somehow sponsored by or affiliated with Microsoft.

9. Given Defendants' apparent willingness to violate the court's orders on an ongoing basis, and the ease and speed with which Defendants can register new IP addresses to continue their attacks, an ongoing process is needed to efficiently and quickly curtail such activities as soon as Defendants register IP addresses for their attacks. Without such a process, Defendants will be able to continue their malicious and illegal activities, will continue to cause irreparable injury to Plaintiffs', their customers and the public. Without such a process, Defendants will not be deterred from engaging in such illegal and harmful activities. I have reviewed the process set forth in the proposed supplemental injunction order submitted with this declaration. Based on my experience and background, I conclude as a technical and practical

matter that the process set forth in the proposed order would enable Plaintiffs and the Court to effectively and efficiently enforce the Court's prior and ongoing orders and stop the irreparable harm caused by Defendants' illegal activities on an ongoing basis.

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 20th day of May 2021.

David E. Anselmi