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 (AJI/IDD)

BRIEF IN SUPPORT OF MICROSOFT'S AMENDED MOTION FOR LIMITED AUTHORITY TO CONDUCT DISCOVERY NECESSARY TO IDENTIFY AND SERVE DOE DEFENDANTS

On October 26, 2020, Plaintiffs Microsoft Corp. ("Microsoft") and Financial Services – Information Sharing And Analysis Center, Inc. ("FS-ISAC") (collectively, Plaintiffs") filed a motion for limited authority to conduct discovery necessary to identify and serve Doe Defendants. Dkt. Nos. 41-43. Pursuant to this Court's request, Plaintiffs hereby file this brief in support of its amended motion providing additional information on the scope of requested third party discovery and more narrowly defining the proposed relief required to identify and serve Doe Defendants and incorporates by reference its prior submission.

Plaintiffs' Need for Third Party Discovery from Currently Identified IP Addresses

On October 6, 2020, this Court granted Plaintiffs' *Ex Parte* Temporary Restraining Order ("TRO") to address Defendants' use of particular IP addresses that control the Trickbot botnet and are part of the command and control infrastructure used to continue Defendants' illegal activities. Dkt. No. 28. Through the steps resulting from the Temporary Restraining Order,

Microsoft and FS-ISAC identified a body of IP addresses, both those that existed at the beginning of the case and which were put into place as Defendants attempted to regain control of the botnet, all of which Defendants attempted to use to rebuild the botnet, in order to infect user computers with malicious software, including dangerous ransomware. In addition to the IP addresses listed in the initial motion for TRO, several subsequent IP addresses were addressed in Plaintiffs' Supplemental TRO which was granted on October 14, 2020. Dkt. No. 35. In several cases, third party infrastructure providers disabled new command and control IP addresses that Defendants attempted to use over the last few weeks, based on the general terms of these orders, even if the IP address was not specifically listed.

The foregoing discrete body of IP addresses is collectively referred to herein as the "Trickbot IP addresses." A full list of the Trickbot IP addresses that are the subject of requested discovery is attached hereto as Exhibit 1. This list includes the IP addresses in the TRO, Supplemental TRO and the additional IP addresses disabled by third party infrastructure providers even though not listed in the orders. Plaintiffs have identified email addresses associated with the Trickbot IP addresses.

Plaintiffs request that this Court grant it the authority to send subpoenas to the third party Internet service providers (ISPs), email service providers, hosting companies, and payment providers associated with the "Trickbot IP addresses" identified in Exhibit 1 which includes the IP addresses in the TRO, Supplemental TRO and the additional IP addresses disabled by third party infrastructure providers even though not listed in the orders at the providers listed in Exhibit 1.

Plaintiffs' Need for Downstream Discovery

Once Plaintiffs undertake third party discovery of the ISPs, email service providers,

hosting companies, and payment providers identified in Exhibit 1, they anticipate that there will be additional targets for discovery when new points of contact, IP addresses, email addresses, methods of payment, etc. are identified. For example, after receiving information about email accounts and IP address accounts used by Defendants and listed in Exhibit 1, there will likely be additional secondary email addresses, login IP addresses, account creation IP addresses and payment information that are identified. All of this information is specifically associated with the Defendants and with the discrete body of Trickbot IP addresses used by Defendants. Plaintiffs request the ability to send further subpoenas to third party providers associated with this information, in their effort to more specifically identify Defendants and to obtain further contact information to provide them notice of the case and to serve the pleadings. Even though the requested discovery is iterative, it will always be related to the original body of Trickbot IP addresses.

In pursuing downstream discovery, Plaintiffs acknowledge the burden that such a sustained effort of requesting relief for each additional target of third party discovery would place on the Court. Plaintiffs therefore propose that if they identify additional third party Internet service providers (ISPs), email service providers, hosting companies, and payment providers from the discovery above, limited to those flowing from the Trickbot IP addresses, they shall be permitted to send further subpoena requests without seeking additional relief from this Court.

Plaintiffs' Future Supplemental TROs

Defendants have continued to put into operation new Trickbot IP addresses throughout the course of this case, and Plaintiffs expect that they may need to seek future Supplemental Orders through the Court Monitor process set forth in the Preliminary Injunction. Dkt. No. 38.

To the extent that new Trickbot IP addresses become part of the case through such Supplemental Orders or informal assistance of third parties in furtherance of the Preliminary Injunction, Plaintiffs request the right to pursue discovery regarding such additional IP addresses and associated email addresses and infrastructure as well. To avoid further burden on this Court, Plaintiffs respectfully request that if such new IP addresses and associated email addresses and infrastructure are identified, that the Plaintiffs shall notify this Court and in a brief pleading apply to supplement the Exhibit 1 discovery targets set forth herein.

CONCLUSION

For the reasons set forth herein, Plaintiffs respectfully request that this Court grant the third party discovery requested in its proposed order.

Dated: October 29, 2020

Respectfully submitted,

/s/ Julia Milewski

Julia Milewski (VA Bar No. 82426)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Telephone: (202) 624-2500
Fax: (202) 628-5116
jmilewski@crowell.com

Gabriel M. Ramsey (*pro hac vice*)
Kayvan M. Ghaffari (*pro hac vice*)
Jacob Canter (*pro hac vice*)
CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111
Telephone: (415) 986-2800
Fax: (415) 986-2827
gramsey@crowell.com
kghaffari@crowell.com
jcanter@crowell.com

Richard Domingues Boscovich (*pro hac vice*)
MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052-6399
Telephone: (425) 704-0867
Fax: (425) 936-7329
rbosco@microsoft.com

Attorneys for Plaintiffs Microsoft Corp. and FS-ISAC, Inc.

EXHIBIT 1

IP addresses as associated with the Trickbot botnet:

104.161.32.10	162.216.0.163	195.123.242.89
104.161.32.101	23.239.84.132	184.164.146.123
104.161.32.102	23.239.84.136	195.123.242.101
104.161.32.103	107.174.192.162	195.123.242.102
104.161.32.105	107.175.184.201	107.155.137.2
104.161.32.106	139.60.163.45	156.146.37.129
104.161.32.109	156.96.46.27	66.115.169.214
104.161.32.112	195.123.241.13	37.235.103.122
104.161.32.118	195.123.241.55	45.131.210.220
104.161.32.125	162.247.155.165	
104.193.252.221	184.164.137.163	
107.155.137.19	192.243.102.123	
107.155.137.28	195.123.242.250	
107.155.137.7	195.123.242.254	

Third-party service providers, hosts, data centers associated with Trickbot IP addresses:

Cloud Equity Group LLC
Cologix, Inc.
Conseev LLC
Datacamp Limited
Equinix, Inc.
Fastlink Network, Inc.
Green Floid LLC
Hosting Solution Ltd.
Hostkey USA, Inc.
Hurricane Electric LLC
Input Output Flood, LLC
Nodes Direct Holdings, LLC
Performive LLC
Phoenix NAP, LLC
Secured Servers LLC
Spin Servers
Twinservers Hosting Solutions, Inc.
Virtual Machine Solutions LLC
VolumeDrive, Inc.
Webair Internet Development Company, Inc.

Google LLC
Oath Holdings Inc.
Paypal Holdings Inc.