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 MOTION FOR LIMITED AUTHORITY TO CONDUCT DISCOVERY NECESSARY TO IDENTIFY AND SERVE DOE DEFENDANTS

Plaintiffs Microsoft Corp. ("Microsoft") and FS-ISAC, Inc. ("FS-ISAC") (collectively, "Plaintiffs") respectfully request an order authorizing them to conduct discovery necessary to identify and to serve the Doe Defendants.

On October 6, 2020, the Court granted an emergency *ex parte* temporary restraining order ("TRO") tailored to halt the activities and the growth and operation of an Internet-based cyber-theft operation referred to as "Trickbot." As set forth in the Court's TRO, the matter involves a network of compromised user computers infected with malware and ransomware, and John Does 1-2 ("Defendants") remotely control these computers using the infrastructure targeted by the Court's TRO. Dkt. No. 28. Prior to issuance of the TRO, Defendants were using the compromised network of computers for the purposes of infecting the computers of Plaintiffs' customers and member organizations, infringing Microsoft's copyrighted software by

reproducing, distributing, and creating derivative works in their malicious software, deceiving victim's by misusing Microsoft's trademarks, and stealing computer users' online login credentials, personal information and highly sensitive and proprietary data. This activity has caused extreme and irreparable injury to Plaintiffs, their customers and member organizations, and the public. Dkt. No. 28.

At present, Plaintiffs are in possession of preliminary information regarding Defendants obtained from *inter alia* public sources of information provided by hosting providers, data centers, and other service providers whose services Defendants used. While much of such information provided in such records appears to be fictitious, Plaintiffs possess information regarding email addresses and IP addresses that Plaintiffs have gathered through their own investigation and from third parties that provide leads to be pursued through discovery tailored to identify Defendants.

In order to identify Defendants from information such as email addresses and IP addresses, it will be necessary to send subpoenas to third party Internet service providers (ISPs), email service providers, hosting companies, and payment providers to obtain account and user information provided by Defendants in association with such email addresses and IP addresses. For example, such service providers often maintain billing and account information identifying the purchasers and account holders of such services, and maintain IP address logs, including data flow analyses, server logs, traffic logs, and any other similar information, associated with the IP address, reflecting the computers from which Defendants logged into their accounts. Given that the account and user information kept by these third-party internet service providers regarding Defendants is generally non-public, the service providers are not likely to provide it to Plaintiffs absent a subpoena.

Plaintiffs, accordingly, request an order granting authority to serve subpoenas and/or international discovery requests to ISPs, third party email service providers, hosting companies, and payment providers to pursue the identities of the Defendants. By the instant motion, Plaintiffs request authority to conduct discovery into these sources to identify Defendants. Given the state of the information currently in Plaintiffs' possession, Plaintiffs believe that limited discovery will assist Plaintiffs in their endeavor to identify, name, and serve Defendants.

I. ARGUMENT

Under Federal Rule of Civil Procedure 26(d), discovery may not normally begin "before the parties have conferred as required by Rule 26(f)." Because Doe Defendants in this case are unknown to Plaintiffs, the conference Rule 26(f) contemplates cannot occur. This limitation on the initiation of discovery, however, can be we waived under Rule 26(d) by Court order.

Courts recognize that, in certain situations, the identity of the defendant may not be known prior to the filing of a complaint. In such circumstances, courts authorize a plaintiff to undertake discovery to identify the unknown defendants. In *Gordon v. Leeke*, 574 F.2d 1147, 1152 (4th Cir. 1978), the Fourth Circuit explained that, if a plaintiff states a meritorious claim against an unknown defendant, the Court should allow plaintiff to ascertain the identity of the unknown defendant through discovery. Courts in this Circuit have also recently authorized parties to conduct discovery based on computer IP addresses, in order to assist in the identification of Doe defendants. *See Arista Records LLC v. Does 1-14*, 2008 U.S. Dist. LEXIS 102974 (W.D. Va. 2008) (granting discovery to identify John Does based on IP addresses); *Virgin Records America, Inc. v. John Doe*, 2009 U.S. Dist. LEXIS 21701 (E.D.N.C. 2009) (same).

This Court has granted Doe discovery used to identify registrants of Internet domains

supporting a botnet in prior cases. In *Microsoft v. John Does 1-8*, Case No. 1:14-cv-00811-LOG/TCB (E.D. Va. 2014), the court recognized the benefit of such discovery and ordered similar discovery so that Microsoft could investigate the identities of registrants of a number of Internet domains used to perpetuate the harmful "Shylock" Botnet. *See* Dkt. No. 39; *see also* Dkt. No. 26 in *Microsoft Corporation v. John Does 1-2*, Case No. 1:20-cv-730 (O'Grady, J.); Dkt. No. 40 in *Microsoft v. John Does 1-27,* Case No. 1:10-cv-00156 (Anderson, J.); Dkt. No. 30 in *Microsoft v. Piatti et al*., Case No. 1:11-cv-1017 (Cacheris. J.). Likewise, in the instant matter, it is appropriate to grant Plaintiffs authority to conduct limited discovery to identify Defendants. Plaintiffs seek a limited discovery period of 180 days, during which it will move forward diligently with subpoenas to ISPs, third-party email providers, payment providers, and web hosting companies in an attempt to further identify Defendants and/or to obtain additional contact information through which to effect service of process.

II. CONCLUSION

For the reasons set forth herein, Plaintiffs respectfully request permission under Rule 26(d) to conduct such discovery for a period of 180 days, as may be necessary, to further identify and serve Defendants.

Dated: October 26, 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.