IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

MICROSOFT CORPORATION, a Washington corporation, FS-ISAC, INC., a Delaware Corporation, HEALTH-ISAC, INC., a Florida corporation, Plaintiffs, v. DENIS MALIKOV, and JOHN DOES 1-7, Defendants.	)	Civil Action No: 1:22-cv-1328-MHC

PLAINTIFFS' MEMORANDUM OF FACT AND LAW IN SUPPORT OF THEIR MOTION FOR LEAVE TO CONDUCT JOHN DOE DISCOVER

Microsoft Corporation ("Microsoft)"), FS-ISAC, Inc. ("FS-ISAC"), and Health-ISAC, Inc. ("Health-ISAC") (collectively "Plaintiffs") file this Motion for Leave to Conduct Jon Doe Discover and Memorandum of Fact and Law in Support Thereof.

On April 8, 2022, the Court granted an emergency *ex parte* temporary restraining order ("TRO") tailored to halt the activities and the growth and operation of a malicious network of computers controlled by a group of actors known as "ZLoader." As set forth in the Court's TRO, the matter involves a network of compromised user computers infected with malware, and Defendants

Denis Malikov and John Does 1-7 ("Defendants") remotely control these computers using the infrastructure targeted by the Court's TRO. Dkt. 27. Prior to issuance of the TRO, Defendants were using the compromised network of computers for the purposes of infecting the computers of Plaintiffs', deceiving them by misuse of Plaintiffs' 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', its customers, and the public. *Id.*

At present, Plaintiffs are in possession of preliminary information regarding Doe Defendants obtained from public sources of information provided by Internet Service Providers ("ISPs"), registries, and other service providers whose services Doe Defendants used, such as email addresses and domains associated with the Defendants. Although some of this information may be fictitious, this information provides Plaintiffs with leads to pursue through formal discovery tailored to identify Doe Defendants.

In order to identify Doe Defendants from information such as email addresses and domain names, it will be necessary to send subpoenas the domain registrars, email service providers, and other internet services and infrastructure providers to obtain account and user information provided by Defendants. 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 reflecting the computers from which Defendants logged into their accounts. This information in turn will allow Plaintiffs to attempt to identify downstream, third party ISPs, email service providers, hosting companies, and payment platforms also used by Defendants in connection with their unlawful activities. 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 conduct Doe Discovery so that Plaintiffs can serve limited subpoenas to third party domain name registrars, third party ISPs, hosting companies, and payment platforms, to pursue the identities of the Defendants. Given the state of the information currently in Plaintiffs' possession, Plaintiffs believe that limited discovery will assist Plaintiffs in its endeavor to identify, name, and serve Doe Defendants.

Accordingly, Plaintiffs respectfully requests that this Court allow such discovery on the terms set forth in the proposed order filed concurrently.

FACTS

I. OVERVIEW OF THE JOHN DOE DEFENDANTS' WRONGFUL ACTS

This lawsuit arises from, among other actionable offenses, Defendants' hosting of a cybercriminal operation, which causes unlawful intrusion into Plaintiffs customers' and member organizations' computers and computing devices and intellectual property violations to the injury of Plaintiffs and Plaintiffs' customers and members organizations. Doe Defendants work in concert to grow, control, and profit from a botnet architecture called ZLoader. ZLoader is made up of computing devices connected to the Internet that Defendants have infected with malicious software (referred to as "malware") that places them under the control of those who utilize the infected devices to conduct illegal activity including to distribute crippling ransomware. Doe Defendants control ZLoader through a command and control infrastructure ("ZLoader Commander and Control Servers") including servers located at the domains subject to the TRO.

The Defendants use the ZLoader botnet through servers connected to the Internet to infect computers in order to extort and steal millions of dollars from unsuspecting victims. The Defendants targets Plaintiffs' customers and members, including end users who use Microsoft's operating system, financial institutions whose customers are stolen from, and health care institutions who are targeted by

ransomware. ZLoader malware, constituting the ZLoader botnet, is disseminated via malicious advertisements, exploits, spam email and spearphishing campaigns, among other methods. The spam email and spearphishing campaigns send unsolicited messages that deceive targeted victims into downloading the ZLoader malware from malicious websites or through malicious attachments, such as those designed to look like legitimate Microsoft Word or Excel files. Once the Defendants caused enough computers to be infected with the ZLoader malware, the Defendants built a scaled ZLoader botnet through which they carry out their illegal acts.

The Defendants also use the ZLoader botnet to install financial theft malware which enables them to ultimately steal money directly from these individuals' bank accounts, as well as to steal personal information from the owners of the infected computers, encrypt the computers with ransomware and demand a ransom or to engage in other malicious activity directed at these victims. The user is unaware of the compromise or other criminal activity as the Defendants have designed ZLoader malware to hide itself and its unlawful activity on infected computers. The Defendants target financial institutions that are members of FS-ISAC through their distribution and use of financial theft malware. The

Defendants target health care institutions that are members of H-ISAC through their distribution and use of ransomware.

Among ZLoader's techniques for stealing victims' credentials and other information is a technique called "webinject," sometimes also referred to as a "man-in-the-browser" attack. This technique is designed to monitor a victim's activity on the infected device and identify and exfiltrate cookies and credentials from browsers and Microsoft Outlook. The ZLoader malware detects when the victim is navigating via their browser to the online portals of a wide variety of financial institutions (members of FS-ISAC), including banks, brokerage firms and credit card companies, and then steals the credentials used for those portals. When ZLoader detects that the user of an infected device is navigating to an online banking website (or any other website specified in the configuration files), the malicious software may do one of the following: (1) access the real banking website (but unbeknownst to the user, execute instructions that modify of extend the website to seek, for example, additional identifying information) or intercept the request from the user's web browser and present the user with a fake website (which appears to be legitimate). Although the victim believes that they are at the legitimate online financial website, they are seeing a version of the website that has been manipulated by the Defendants. When the user types their login credentials

into the fake website or the fraudulent fields injected by the Defendants, the Defendants are able to intercept that information and use it to log into the user's online accounts. The Defendants can then initiate funds transfers, resulting in theft of the victim's money.

Doe Defendants' wrongful acts misappropriate Plaintiffs' name, marks, and intellectual property and defraud the American public. Plaintiffs have not authorized any Defendant to use in any way its name or marks. Moreover, Plaintiffs are in no way affiliated with any Defendant.

II. DEFENDANTS' CONCEALMENT OF THEIR IDENTITIES

As a fundamental and necessary aspect of the Defendants' activities, the Doe Defendants go through great lengths to minimize the likelihood that their identities are revealed. For example, Doe Defendants purposefully communicate and transact business exclusively by electronic means. Defendants conceal their identities and physical contact information and locations in an effort to avoid liability for their illegal conduct. The Doe Defendants take steps not to reveal their name or true contact information. However, in creating the ZLoader infrastructure, Doe Defendants provided certain identifying information to various third-party service providers. By conducting Doe Discovery, Plaintiffs anticipate obtaining

additional points of contact that may allow Plaintiffs to determine Defendants' true identities.

III. PLAINTIFFS' CURRENT KNOWLEDGE AND INVESTIGATION

Prior to the filing of the present lawsuit on April 6, 2022, Plaintiffs' investigation of Defendants' infringement and other wrongful acts allowed Plaintiffs to discover, through their own investigation and through third parties, preliminary information regarding the Doe Defendants, such as email addresses and domain names that have been used in connection with these Defendants' activities. Without the aid of John Doe discovery taken under the color of the present lawsuit, Plaintiffs will not be able to use the information such as email addresses, domain names, and IP addresses to identify Doe Defendants with the requisite degree of certainty necessary: (1) for their inclusion as specifically named defendants herein, (2) for the successful prosecution by Plaintiffs of their claims herein; and (3) for the protection by Plaintiffs' of their infringed-upon marks.

ARGUMENT

I. JOHN DOE DISCOVERY – GENERALLY

Federal Rule of Civil Procedure 26(d)(1) permits a party to conduct discovery in advance of the conference of parties required by Fed. R. Civ. P. 26(f), "when authorized by these rules, by stipulation, or by court order." Fed. R. Civ.

P.26(d)(1). The federal judiciary has repeatedly recognized the utility and efficacy of using "John Doe" discovery methods to establish the identities of unknown wrongdoers and to defeat their attempts to avoid responsibility for their criminal acts. *See, e.g., Verizon Online Services v. Ralsky*, 203 F. Supp. 2d 601, 609 n.5 (E.D. Va. 2002). Courts in this district have specifically allowed John Doe discovery similar to the Doe discovery Plaintiffs are requesting here. *See, e.g.*, *Delta Air Lines, Inc. v. John Does 1-25*, No. 17-cv-3671 (Dkt. 5) (N.D. Ga. Nov. 2, 2017); *Delta Air Lines, Inc. v. John Does 1-50*, No. 13-cv-3388, slip op. (Dkt. 3) (N.D. Ga. Oct. 28, 2013).

II. PLAINTIFFS' PROPOSED DISCOVERY

Plaintiffs' proposed discovery includes at least the following major steps. Because the Doe Defendants have concealed their identities and sometimes used multiple intermediates to do so, Plaintiffs anticipate that it will be necessary to send somewhat iterative discovery that, in general, is first designed to uncover the Doe Defendants true identity and/or use of other Internet providers to facilitate their involvement in ZLoader, and then to obtain further specific information about the Doe Defendants.

A. Domain Registrars

Plaintiffs intend to serve subpoenas to the domain registrars that Plaintiffs have identified as being associated with the Defendants' unlawful activity and were used to register the domain names that are subject to the TRO ("ZLoader Domains"). Should the Court grants Plaintiffs' request for Doe discovery, Plaintiffs currently intend to subpoena the following domain registrars:

Dynadot, LLC	Real Time Register B.V.
Registrar Of Domain Names REG.RU LLC	TUCOWS, Inc.
Big Rock Solutions Ltd.	Fastdomain, Inc.
Namecheap, Inc.	Godaddy.Com, LLC
123-Reg Limited	Pdr Ltd. D/B/A Publicdomainregistry.Com
Touchdown Domains LLC	Hosting Ukraine LLC
Cv. Rumahweb Indonesia	Namesilo, LLC
Register.Ca Inc.	Domain Original, LLC
Dropcatch.Com 1508 LLC	Domain.Com, LLC.
Hosting Concepts B.V. D/B/A Registrar.Eu	Eranet International Limited
WEBCC Web Commerce Communications Limited Dba Webnic.Cc	Snapnames 73, LLC
Launchpad, Inc. (Hostgator)	Google LLC
Internet Domain Service Bs Corp.	Eranet International Limited
Regional Network Information Center, JSC Dba RUCENTER	GMO Internet, Inc.
PDR Ltd. D/B/A Publicdomainregistry.Com	

Information obtained from the domain registrars will establish additional points of contact with the Doe Defendants, allowing Plaintiffs to ensure notice is

effectuated to the fullest scope possible and potentially allowing Plaintiffs to establish the identity of the Doe Defendants.

B. Email Service Providers

Plaintiffs also intend to serve subpoenas to the email service providers that Plaintiffs have identified as being associated with the Defendants and were used to register the ZLoader Domains. Should the Court grants Plaintiffs' request for Doe discovery, Plaintiffs currently intend to subpoena the following email service providers:

Yahoo Inc.	WithheldForPrivacy	Contactprivacy.com
Google LLC	DomainDiscreet	PrivacyProtected.net
DomainDataGuard	PrivacyGuardian	SafeWhoIs
Zwoho	HugeDomains	DomainsbyProxy.com
Mailernam	Whoisprivacycorp	Onamae.com
WhoIsProtectService		

Information obtained from the email service providers will establish additional points of contact with the Doe Defendants, also allowing Plaintiffs to ensure notice is effectuated to the fullest scope possible and potentially allowing Plaintiffs to establish the identity of the Doe Defendants.

C. Downstream Third Parties: Internet Service Providers, Hosting Companies, and Payment Processors.

Once Plaintiffs undertake third party discovery of the domain registrars and email service providers, Plaintiffs anticipate that there will be additional targets for

discovery when new points of contact, IP addresses, email addresses, methods of payment, hosting companies, internet service providers, and payment processors used by the Doe Defendants are identified. For example, after receiving information from the domain registrars and email service providers about the email accounts used by the Doe Defendants, there will likely be additional secondary email addresses, login IP addresses, account creation IP addresses and payment information that are identified as being associated with the Doe Defendants. All of this information will be specifically associated with the Defendants and with the discrete body of ZLoader Domains used by Defendants. Plaintiffs request the ability to send further subpoenas to further third party providers associated with information obtained during Doe discovery, in their effort to more specifically identify the Doe 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 somewhat iterative, it is not unbounded and will always be related to the original body of ZLoader Domains that were subject to the TRO and to the purpose of identifying the true identity of the Doe Defendants.

In pursuing downstream discovery, Plaintiffs acknowledge the burden that such a sustained effort of requesting relief from the Court for each additional target of third-party discovery would place on the Court. Plaintiffs therefore propose that

if they identify additional third party ISPs, email service providers, hosting companies, payment providers, or other Internet providers from the specifically delegated Doe discovery described above, limited to those flowing from the ZLoader domains, Plaintiffs shall be permitted to send further subpoena requests as part of the Doe discovery without seeking additional relief from this Court each time.

CONCLUSION

For the foregoing reasons, Plaintiffs respectfully request that their motion to conduct John Doe discovery be granted. A proposed order is being filed with this Motion for the Court's convenience.

Dated: May 4, 2022

Respectfully submitted,

/s/ Joshua D. Curry
Joshua D. Curry

Joshua D. Curry (Georgia Bar No. 117378)
Jonathan D. Goins (Georgia Bar No. 738593
LEWIS BRISBOIS BISGAARD & SMITH LLP
600 Peachtree Street NE, Suite 4700
Atlanta, GA 30308
Tel: 404.348.8585
Fax: 404.467.8845
josh.curry@lewisbrisbois.com
jonathan.goins@lewisbrisbois.com

Gabriel M. Ramsey (*pro hac vice*)
Anna Z. Saber (*pro hac vice*)

CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111
Tel: (415) 986-2800
Fax: (415) 986-2827
gramsey@crowell.com
asaber@crowell.com

Emily Alban (*pro hac vice*)
Garylene Javier (*pro hac vice*)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Tel: (202) 624-2500
Fax: (202) 628-5116
ealban@crowell.com
gjavier@crowell.com

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

Attorneys for Plaintiff Microsoft Corporation

CERTIFICATION OF COMPLIANCE

Pursuant to L.R. 7.1(D), N.D. Ga., counsel for Plaintiff hereby certifies that this Motion has been prepared with one of the font and point selections approved by the Court in L.R. 5.1, N.D. Ga.

Dated: May 4, 2022

Respectfully submitted,

/s/ Joshua D. Curry
Joshua D. Curry