

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

MICROSOFT CORPORATION, a)
Washington corporation,)
)
Plaintiff,) Civil Action No: 1:21-cv-01346 (LMB/TCB)
)
v.)
)
JOHN DOES 1-2, CONTROLLING)
A COMPUTER NETWORK AND)
THEREBY INJURING PLAINTIFF)
AND ITS CUSTOMERS,)
)
Defendants.)
)
)
)
)

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

Plaintiff Microsoft Corp. (“Microsoft”) respectfully requests an order authorizing it to conduct discovery necessary to identify and to serve the Doe Defendants.

On December 2, 2021, the Court granted an emergency *ex parte* temporary restraining order (“TRO”) tailored to halt the operation and growth of an Internet-based cyber-crime operation referred to as “Nickel.” As set forth in the Court’s TRO, the matter involves a criminal network that are engaged in illegally accessing the accounts and computer networks of Microsoft’s customers and stealing highly sensitive information. Dkt. No. 04. To manage and direct Nickel, Defendants established and operate a network of websites, domains, and computers on the Internet, which they use to target their victims, compromise their online accounts, infect their computing devices, compromise the security of their networks, and steal sensitive information from them. John Does 1-2 (“Defendants”) remotely control the

domains that compromise the infected users using infrastructure targeted by the Court's TRO.

Prior to issuance of the TRO, the Defendants compromise victims' computers by installing malware to obtain account credentials to later retrieve sensitive communications within the accounts. *See* Declaration of Christopher Coy in Support of Motion for Temporary Restraining Order ¶¶ 8-9. Dkt. No. 8. The accounts are a part of the compromised network of computers targeting government employees, organizations, and individuals working on a myriad of foreign diplomacy issues, think tanks, members of organizations that attempt to maintain world peace, human rights organizations, as well as many other organizations and individuals. *Id.* ¶ 7. Defendants use malware to compromise virtual private network ("VPN") appliances and after entering a network, searches for data or assets to exfiltrate, moving through the compromised environment and obtaining increased privileges. *Id.* ¶ 9, 13. This activity has caused extreme and irreparable injury to Microsoft, its customers, and the public.

At present, Microsoft is in possession of limited, preliminary information regarding Defendants obtained from *inter alia* public sources of information provided by domain registries and registrars and other service providers whose services Defendants used. While much of such information provided in such records appears to be fictitious, Microsoft possesses information regarding email addresses associated with Defendants that Microsoft has gathered through its own investigation. The domain names and these email addresses provide leads to be pursued through discovery tailored to identify Defendants.

In order to identify Defendants from information such as email addresses, domain names and IP addresses, it will be necessary to send subpoenas to third party email service providers, domain registrars, hosting companies and payment providers to obtain account and user information provided by Defendants in association with such email addresses, domain names 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 associated with Defendants or their access to services, including data flow analyses, server logs, traffic logs, and any other similar information, associated with the IP addresses, 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 Microsoft absent a subpoena.

Microsoft, accordingly, requests an order granting authority to serve subpoenas and/or international discovery requests to third party email service providers, domain name registrars, hosting companies and payment providers, to pursue the identities of the Defendants. By the instant motion, Microsoft requests authority to conduct discovery into these sources to identify Defendants. Given the state of the information currently in Microsoft's possession, Microsoft believes that limited discovery will assist Microsoft in its 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 Microsoft, the conference Rule 26(f) contemplates cannot occur. This limitation on the initiation of discovery, however, can be 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 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 cybercrime 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 Microsoft authority to conduct limited discovery to identify Defendants.

Microsoft seeks a limited discovery period of 180 days, during which it will move forward diligently with subpoenas to email service providers, domain name registrars, hosting companies and payment providers in an attempt to further identify Defendants and/or to obtain additional contact information through which to effect service of process. The discovery will be narrowly tailored such that it only seeks information that is related to known infrastructure associated with the Defendants. Microsoft’s initial discovery will be directed to the third-party

service providers GoDaddy Inc. (domain registrar), Enom Inc. (domain registrar), and Xinnet Technology Corp. (domain registrar), which are known to be directly or indirectly associated with Defendants and the infrastructure at issue in this case. Once Microsoft undertakes third party discovery of the known email service providers, domain name registrars and hosting companies, associated with Defendants, Microsoft anticipates 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, 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 infrastructure used by Defendants. Microsoft requests 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 infrastructure known to be associated with Defendants.

In pursuing downstream discovery, Microsoft acknowledges 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 known infrastructure of Defendants, they shall be permitted to send further subpoena requests without seeking additional relief from this Court.

II. CONCLUSION

For the reasons set forth herein, Microsoft respectfully requests 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: December 10, 2021

Respectfully submitted,

/s/ David J. Ervin

David J. Ervin (VA Bar No. 34719)

Garylene Javier (*pro hac vice*)

CROWELL & MORING LLP

1001 Pennsylvania Avenue NW

Washington DC 20004-2595

Telephone: (202) 624-2500

Fax: (202) 628-5116

dervin@crowell.com

gjavier@crowell.com

Gabriel M. Ramsey (*pro hac vice*)

Kayvan Ghaffari (*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

Attorneys for Plaintiffs Microsoft Corp.

CERTIFICATE OF SERVICE

I hereby certify that on December 10, 2021, I will electronically file the foregoing with the Clerk of Court using the CM/ECF system.

Copies of the foregoing were also served on the defendants listed below by electronic mail:

John Does 1-2

c/o

benbasta@tutanota.com
tatanotakeeps@tutanota.com

/s/ David J. Ervin

David J. Ervin (VA Bar No. 34719)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Telephone: (202) 624-2500
Fax: (202) 628-5116
dervin@crowell.com

Attorney for Plaintiff Microsoft Corp.