ORAL ARGUMENT REQUESTED

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MICROSOFT CORPORATION, a Washington Corporation, FORTRA, LLC, a Delaware Limited Liability Company, and HEALTH-ISAC, INC., a Florida Corporation,

Plaintiffs,

v.

JOHN DOES 1-2, JOHN DOES 3-4 (AKA CONTI RANSOMWARE GROUP), JOHN DOES 5-6 (AKA LOCKBIT RANSOMWARE GROUP), JOHN DOES 7-8 (AKA DEV-0193), JOHN DOES 9-10 (AKA DEV-0206), JOHN DOES 11-12 (AKA DEV-0237), JOHN DOES 13-14 (AKA DEV-0243), JOHN DOES 15-16 (AKA DEV-0504), Controlling Computer Networks and Thereby Injuring Plaintiffs and Their Customers,

Defendants.

Case No. 1:23-cv-2447-LDH-JRC

FILED UNDER SEAL

BRIEF IN SUPPORT OF PLAINTIFFS' *EX PARTE* MOTION FOR A SECOND SUPPLEMENTAL PRELIMINARY INJUNCTION ORDER

Plaintiffs Microsoft Corporation ("Microsoft"), Fortra, LLC ("Fortra"), and Health-ISAC, Inc., ("H-ISAC") seek an *Ex Parte* Second Supplemental Preliminary Injunction Order to address Defendants' continuing efforts to rebuild the Cracked Cobalt Strike command and control infrastructure and continue their illegal activities in open defiance of this Court's Preliminary Injunction Order and First Supplemental Preliminary Injunction Order. Plaintiffs express their appreciation for the continued attention of the Court to this ongoing cyber-security matter.

Plaintiffs incorporate by reference herein the arguments and evidence set forth in their Brief In Support Of Plaintiffs' Application for an *Ex Parte* Temporary Restraining Order and Order To Show Cause Re Preliminary Injunction ("TRO Application"), Dkt. No. 3, and Brief In Support of

Plaintiffs' *Ex Parte* Motion to Supplement the Preliminary Injunction Order ("First Supplemental Preliminary Injunction Motion"), Dkt. No. 23-5. As discussed in Plaintiffs' TRO Application and First Supplemental Preliminary Injunction Motion, the domains used in cracked Cobalt Strike's command and control infrastructure are critical to the operation conducted by John Does 1-16 (collectively "Defendants") whereby Defendants have abused the legitimate security testing tool known as Cobalt Strike for illegal and malicious purpose that causes extreme and continued irreparable harm to Plaintiffs, their customers and members, as well as the general public. The most effective way to disrupt Defendants' operation is to disable the domains used by Defendants in connection with the various instances of cracked Cobalt Strike.

I. BACKGROUND

On March 31, 2023, the Court granted and Emergency *Ex Parte* Temporary Restraining Order ("TRO") tailored to halt the illegal activities and the growth of Defendants' cracked Cobalt Strike Operation. Dkt. No. 13. Defendants' use cracked versions of Cobalt Strike to deploy malware and ransomware onto victims' computers, allowing Defendants to infect victims' computers, hijack the victims' operating systems, and steal users' sensitive data. Defendants cause great harm to Plaintiffs by damaging the products and services they provide to their customs. Further, by exploiting Plaintiffs' famous and highly-regarded trademarks, products, and services to disguise and further its criminal conduct, Defendants cause Plaintiffs irreparable reputational and other harms for which no monetary recourse is available.

As explained in Plaintiffs' TRO Application, Defendants conduct their illegal operations by using an online command and control infrastructure consisting of a set of websites and domains. Dkt. No. 3-1 at 6. These domains are used both to break into computers and networks of the organizations that Defendants targets, perform reconnaissance of those networks, and, ultimately, exfiltrate sensitive information from them. To disable this command and control infrastructure,

this Court ordered that these Defendants-controlled domains, listed in Appendix A filed on March 30, 2023, be redirected to secure Microsoft servers. Dkt. No. 13. On April 19, 2023, the Court converted the TRO into a Preliminary Injunction. Dkt. No. 20. On May 15, 2023, Plaintiffs filed a Motion for Expedited Discovery to Identify Doe Defendants. Dkt. No. 21. The Motion for Expedited Discovery remains pending, and Plaintiffs have not been able to endeavor to identify the Doe Defendants and Doe Defendants continue to demonstrate their technical sophistication through the rebuilding of the cracked Cobalt Strike command and control infrastructure. On June 16, 2023, the Court granted Plaintiffs' First Supplemental Preliminary Injunction Motion. Dkt No. 24.

Through executing the Court's Temporary Restraining Order, Preliminary Injunction Order, and First Supplemental Preliminary Injunction Order, Plaintiffs cut communications between Defendants' existing command and control infrastructure and the victim computers and networks that Defendants attacked and from which Defendants had been stealing information. Declaration of Derek Richardson In Support Of Plaintiffs' Motion for a Second Supplemental Preliminary Injunction Order ("Richardson Decl.") ¶¶ 7-8. This effectively stymied Defendants' effort to exploit the computers and networks they had targeted or compromised. *Id.*

However, Defendants, who are evidently resourceful and well-funded, continue to try to maintain and reestablish new command and control domains and other command and control infrastructure so that they can continue their illegal activities. *Id.* ¶¶ 9-10. Indeed, this probability was foreseen by the Court in issuing its TRO. And as foreseen, following the execution of the TRO and Preliminary Injunction, as well as the First Supplemental Preliminary Injunction, Defendants openly defied this Court and started to rebuild their command and control infrastructure by adding 15 new domains to the cracked Cobalt Strike command and control

infrastructure. *Id.* ¶ 9. Consequently, Plaintiffs ask the Court to allow it to redirect the new domains associated with the cracked Cobalt Strike operation to Microsoft secure servers. *Id*. ¶¶ 11-13. This will disrupt Defendants' recent illegal activity. A list of the new domains used by Defendants is provided in Appendix A to the Proposed Order filed concurrently with this brief.

II. ARGUMENT

A. There Is Good Cause to Supplement the Preliminary Injunction Order

Plaintiffs seek to further supplement the Preliminary Injunction Order by including the domains in Appendix A to the Proposed Order submitted with this motion to the prior list of domains transferred to Microsoft pursuant to the Court's prior injunctive relief. This will allow Plaintiffs to disrupt Defendants more recent illegal activity. Such supplemental relief has been granted in prior cases when defendants began using new domains after the court granted a temporary restraining order. *See, e.g.*, *Microsoft Corp. v. John Does 1-8*, Case No. l:14-cv-00811-LOG-TCB (E.D. Va. 2014) (O'Grady, J.) at Dkt. No. 32 (supplemental injunctive relief aimed at disabling the "Shylock" botnet); *Microsoft Corp. v. John Does 1-2*, Case No. 1:19-cv-00716-ABJ (Berkman Jackson, J.) at Dkt. No. 21 (granting supplemental injunction to seize additional domains associated with the Phosphorous command and control infrastructure). Here, absent the requested relief, irreparable harm will continue to Plaintiffs and their customers, for the reasons detailed in Plaintiffs' prior submissions. Plaintiffs are likely to succeed on the merits, because the domains at issue in this motion are used for the same unlawful purposes and in the same unlawful manner set forth in Plaintiffs' previous TRO Application and First Supplemental Preliminary Injunction Motion. Richardson Decl. ¶ 10. Thus, pursuant to Federal Rule of Civil Procedure 65, disabling the additional 56 domains at issue is necessary to prevent harm to Plaintiffs and their customers. With respect to supplementing the Preliminary Injunction Order, *ex parte* relief is essential. If notice is given prior to issuance of the requested relief, it is likely that Defendants will be able to

quickly mount an alternate command and control structure because Defendants have the technical sophistication and ability to move their malicious infrastructure. Richardson Decl. ¶¶ 13-16. Thus, providing notice of the requested *ex parte* relief will undoubtedly facilitate efforts by Defendants to continue to operate. Rule 65 of the Federal Rules of Civil Procedure permits *ex parte* injunctive relief where the moving party sets forth facts that show an immediate and irreparable injury and why notice should not be required. Fed. R. Civ. P. 65(b)(1); *see Granny Goose Foods, Inc. v. Brotherhood of Teamsters & Auto Truck Drivers, Local No. 70*, 415 U.S. 423, 438–39 (1974) ("Ex parte temporary restraining orders are no doubt necessary in certain circumstances…."). It is well established that *ex parte* relief is appropriate under circumstances such as here, where notice would render the requested relief ineffective. *See, e.g.*, *AT&T Broadband v. Tech Commc'ns, Inc.*, 381 F.3d 1309, 1319-20 (11th Cir. 2004) (affirming *ex parte* search and seizure order to seize contraband technical equipment, given evidence that in the past defendants and persons similarly situated had secreted evidence once notice given); *In re Vuitton Et Fils S.A.*, 606 F.2d 1, 4-5 (2d Cir. 1979) (holding that notice prior to issuing TRO was not necessary where notice would "serve only to render fruitless further prosecution of the action"; prior experience taught that once one member of the counterfeiting enterprise received notice, contraband would be transferred to another unknown counterfeiter, perpetuating the harm and rendering judicial efforts pointless); *Little Tor Auto Ctr. v. Exxon Co., USA*, 822 F. Supp. 141, 143 (S.D.N.Y. 1993) (*ex parte* TRO appropriate where contraband "may be destroyed as soon as notice is given").

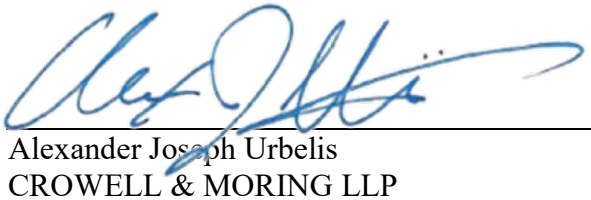
As before in this matter, immediately upon execution of the Second Supplemental Preliminary Injunction Order and disabling of the additional domains addressed in the attached proposed order, Plaintiffs will provide robust notice to the Defendants, consistent with the alternative service methods already authorized by this Court. Dkt. No. 13. Plaintiffs will provide

Defendants the documents associated with this motion and the Court's order, by sending them to all of Defendants' contact information associated with the subject domains, thus providing notice and an opportunity to appear and contest the requested relief, if Defendants so choose.

III. CONCLUSION

For the reasons set forth in this brief, the Richardson Declaration submitted with this brief and based on the evidence submitted with the prior Application for TRO, Preliminary Injunction, and First Supplemental Preliminary Injunction, Plaintiffs respectfully request that the Court grant Plaintiffs' Motion For A Second Supplemental Preliminary Injunction Order.

Dated: September 27, 2023



Alexander Joseph Urbelis
CROWELL & MORING LLP
590 Madison Ave #20th
New York, NY 10022
Telephone: (212) 223-4000
Fax: (212) 223-4134
aurbelis@crowell.com

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

Gabriel M. Ramsey (*pro hac vice*)
Amanda (Anna) Z. Saber (*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
asaber@crowell.com

Richard Boscovich (*of counsel*)
Maria Little (*of counsel*)

MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052-6399
Telephone: (425) 704-0867
Fax: (425) 936-7329

Joseph Belton (*of counsel*)
FORTRA, LLC
11095 Viking Drive, Suite 100
Eden Prairie, MN 55344
Phone: +1 952-933-0609

Attorneys for Plaintiffs Microsoft Corp., Fortra LLC, and H-ISAC, Inc.