PIN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Microsoft Corporation, a Washington State Corporation, NGO-ISAC, a New York State Non-Profit Organization, Plaintiffs, v. John Does 1-2, Controlling A Computer Network and Thereby Injuring Plaintiff and Its Customers, Defendants.	Civil Action No.: 1:24-cv-02719-RC **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5.1**

MEMORANDUM IN SUPPORT OF PLAINTIFFS' FIRST *EX PARTE* MOTION TO SUPPLEMENT THE PRELIMINARY INJUNCTION ORDER

Plaintiffs Microsoft Corporation ("Microsoft") and NGO Information Sharing and Analysis Center ("NGO-ISAC") (collectively "Plaintiffs") by their attorneys, pursuant to Federal Rule of Civil Procedure 65(a) and (c), the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1116, 1125), District of Columbia common law, and the All Writs Act (28 U.S.C. § 1651) seek an *Ex Parte* Supplemental Preliminary Injunction Order to seize additional domains from the Star Blizzard Defendants who continue are rebuilding the Star Blizzard command and control infrastructure to continue their illegal cybercriminal activities in open defiance of this Court's TRO and Preliminary Injunction Order (Dkt. Nos. 12, 20).

Plaintiffs incorporate by reference herein the arguments and evidence set forth in their Memorandum in Support of Plaintiffs' Application for an *Ex Parte* Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Application.") and supporting declarations Dkt. No. 4. As discussed in Plaintiffs' TRO Application, the domains used by the

Star Blizzard Defendants are critical to the operation of the Star Blizzard Defendants' prolific spear phishing[1] campaigns, whereby the Star Blizzard Defendants establish and operate a network of websites, domains, and computers on the Internet, which they use to compromise the security of their victims and steal their sensitive information. Microsoft has identified these new domains and linked them exclusively to Star Blizzard Defendants the exact same way it identified the domains that were subject to this Court's original injunctions. Defendants' continuing conduct causes extreme irreparable harm to Plaintiffs, their customers and member organizations, as well as the general public. The most effective way to disable the Star Blizzard Defendants' criminal operation is to disable the Internet domains they use. Plaintiffs respectfully request that the Court supplement the Preliminary Injunction Order to allow seizure of additional domains to further disable the Star Blizzard criminal organization.

I. BACKGROUND

On September 25, 2024, the Court granted Plaintiffs' Emergency *Ex Parte* Temporary Restraining Order ("TRO") tailored to halt the illegal activities of the Star Blizzard operation. Dkt. No. 12. The Court found that there was good cause to believe that the Star Blizzard Defendants had engaged in violations of the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act, the Lanham Act, and engaged in acts constituting trespass to chattels, conversion, and unjust enrichment. *Id.* at 2. Specifically, the Court found that the Star Blizzard Defendants violate the law by intentionally accessing the protected computers of Microsoft, its customers, including NGO-ISAC, and NGO-ISAC's member organizations, without authorization in order to

[1] Spear phishing, as used by Plaintiffs Microsoft and NGO-ISAC in this action, is a type of personalized attack in which the threat actor or cybercriminal attempts to acquire sensitive information or access a computer by sending a fake email message that appears to be legitimate, with the goal of having the victim interact further with the email (referred to as the "lure"). *See* Dkt. No 4-2 (Declaration of Sean Ensz in Support of Plaintiffs' TRO Application, ("Ensz TRO Decl.") ¶ 5.

steal and exfiltrate information from those computers, engage in a spear phishing operation to steal credentials from unsuspecting victims , and access without authorization the email inboxes of Microsoft and its customers, including NGO-ISAC and NGO-ISAC's member organizations. *Id.* at 3.

As explained in Plaintiffs' TRO Application, the Star Blizzard Defendants conduct their illegal operations by using an online command and control infrastructure consisting of a set of websites and domains. Dkt. No. 4-1 (TRO Application) at 5-11. The Star Blizzard Defendants use these domains to break into computers and networks of the organizations that Star Blizzard Defendants target, perform reconnaissance of those networks, and, ultimately, exfiltrate sensitive information from them. *Id.*

To disable this command and control infrastructure, this Court ordered that these Star Blizzard-controlled domains, listed in Appendix A to the Complaint, be transferred and redirected to secure Microsoft servers. Dkt. No. 12. These domains were successfully transferred to Microsoft's secure servers. On October 10, 2024, the Court converted the TRO into a Preliminary Injunction, thus allowing Microsoft to maintain possession of the seized domains of the Star Blizzard Defendants. Dkt. No. 20.

In executing the Court's Temporary Restraining Order and Preliminary Injunction Order, Microsoft took possession of the Star Blizzard Defendants' domains. This allowed Plaintiffs to cut the communications between the Star Blizzard Defendants' then-existing command and control infrastructure and the victims computers and email accounts that the Star Blizzard Defendants had spear phished and from which the Star Blizzard Defendants had been stealing sensitive personal and business information. *See* Declaration of Sean Ensz In Support of Plaintiffs' Motion to Supplement Preliminary Injunction Order (Ensz Suppl. Decl.) ¶6. This effectively stymied the

Star Blizzard Defendants' efforts to exploit the computers and email accounts that they had already targeted or has successfully spear phished.

The Star Blizzard Defendants, however, are technically sophisticated and resourceful. Dkt. No. 4-3 (Ensz TRO Decl.) ¶ 58 ("The Star Blizzard Defendants' techniques are designed to resist technical mitigation efforts, eliminating the ability to curb the injury purely through technical means. For example, once domains in the Star Blizzard Defendants' active infrastructure become known to the security community, the Defendants abandon that infrastructure and move to new infrastructure that is used to continue Defendants' efforts to compromise accounts of new victims"). The Star Blizzard Defendants evidently are using their technical sophistication and vast resources to move to new infrastructure so that they can continue their illegal activities. Indeed, this probability was foreseen by the Court in issuing the TRO on an *ex parte* basis. Dkt No. 12 (TRO) at 6 ("There is good cause to believe that if the Star Blizzard Defendants are provided advance notice of Plaintiffs' TRO Application or this Order, they would move the Star Blizzard Defendants' infrastructure, allowing them to continue their misconduct . . ."). And as foreseen, following the execution of the TRO and Preliminary Injunction, the Star Blizzard Defendants openly defied this Court and started to rebuild their command and control infrastructure so that they can resume their cybercriminal operations and spear phish additional victims. Ensz Suppl. Decl. ¶ 7. To rebuild their infrastructure, the Star Blizzard Defendants have registered new domains and have reconfigured preexisting, dormant domains. *Id.* In total, the rebuilding efforts includes 75 domains. *Id.* ¶ 9. These domains bear the same unique "signatures" or "digital fingerprints" that allow Plaintiffs to establish with a high level of confidence that these new domains have been registered by the Star Blizzard Defendants to carry out the same criminal activity that the Star Blizzard Defendants have been enjoined from. Dkt. No. 4-2 (Ensz TRO

Decl.) ¶¶ 32, 38-41; *see* also Ensz Suppl. Decl. ¶¶ 10-12. For example, one observed tactic of the Star Blizzard Defendants is that they use fake login pages that appear to look like a legitimate Microsoft login page but in reality, are controlled by the Star Blizzard Defendants and used to intercept and steal credentials. Dkt. No. 4-2 (Ensz TRO Decl.) ¶ 32, Figure 11. The Star Blizzard Defendants employ the same tactic here with respect to the new domains. Login pages associated with these new, Star Blizzard-controlled domains also appear to be legitimate Microsoft login pages, but in fact are fraudulent. *See* Ensz Supp. Decl. ¶¶ 11, Figures 1 and 2.

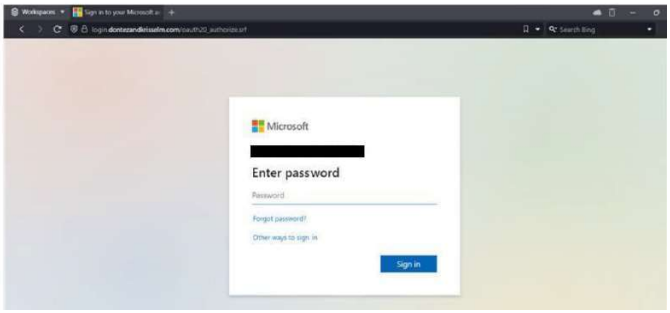

Figure XX

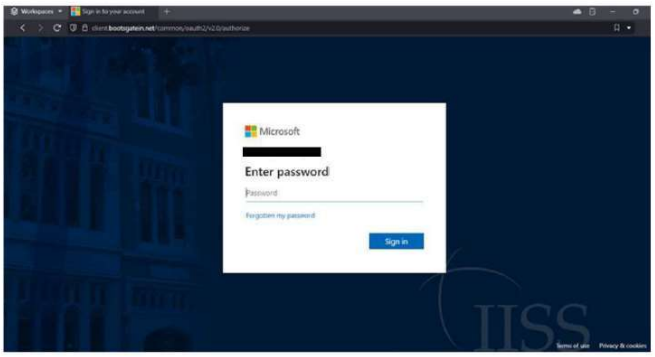

Figure XX

Consequently, Plaintiffs respectfully request the Court to allow Plaintiffs to transfer ownership of the domains and redirect these new Star Blizzard-controlled domains to Microsoft secure servers. Ensz Supp. Decl. ¶¶ 13-16. This will disrupt the Star Blizzard Defendants' recent illegal activity designed to circumvent the TRO. A list of the new domains used by the Star

Blizzard Defendants in their attempts to rebuilt their technical infrastructure 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.

"The Court has power to supplement and modify interlocutory injunctive relief previously granted in order to fit changing circumstances." *Air Transp. Ass'n of Am. v. Hernandez*, No. 3096-66, 1967 WL 97, at *5 (D.D.C May 23, 1967); *see also Trump v. Int'l Refugee Assistance Project*, 582 U.S. 572, 579 (2017) (court may modify injunction using its "equitable discretion.") The party seeking modification of a preliminary injunction order has the burden of establishing "a significant change in circumstances warrants its revisions." *Gov't of Province of Manitoba v. Zinke*, 849 F.3d 1111, 1117 (D.C. Cir. 2017). This can be done through establishing a significant change in either the factual conditions giving rise to the injunction or in law. *New York v. Biden*, No. 20-cv-2340-EGS, 2021 WL 7908124, at *2 (D.D.C. Aug. 23, 2021)

Here, the Star Blizzard Defendants' attempts to rebuild their criminal organization constitute a significant change in the factual conditions that merits modifying the preliminary injunction order to include these additional domains. *Id.* Plaintiffs request that the Court order these additional domains, which are listed in Appendix A to the Proposed Order, be transferred to Microsoft consistent with the methodology authorized in the TRO. *See* Dkt. No. 12 (TRO) at 8-10. This will allow Plaintiffs to disrupt the Star Blizzard Defendants more recent illegal activity. Such supplemental relief has been granted in prior cases when cybercriminal defendants began using new domains after the court granted a temporary restraining order. *See Microsoft Corp. v. John Does 1-2*, Case No. 1:19-cv-00716-ABJ (D.D.C 2019) (Berman Jackson, J.) at Dkt. Nos. 21, 30 (granting supplemental injunctions to seize additional domains associated with the Phosphorous

command and control infrastructure); *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 (disabling the "Shylock" botnet).

Here, absent the requested relief, Plaintiffs will continue to suffer irreparable harm 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 motion for TRO and Preliminary Injunction. Ensz Suppl. Decl. ¶¶ 10-11; *see also* Dkt. No. 12 (TRO) at 2-3. Thus, pursuant to Federal Rule of Civil Procedure Rule 65, disabling the additional 75 domains at issue is necessary to prevent harm to Plaintiffs, their customers and, and their member organizations.

B. <u>There is Good Cause to Grant *Ex Parte* Relief</u>

With respect to supplementing the Preliminary Injunction Order, *ex parte* relief is essential. As addressed at the TRO stage, if notice is given prior to issuance of the requested relief, it is likely that the Star Defendants will be able to quickly mount an alternate command and control structure because the Star Blizzard Defendants have the technical sophistication and ability to move their malicious infrastructure. Ensz Suppl. Decl. ¶¶ 17-18. Thus, providing notice of the requested *ex parte* relief will undoubtedly facilitate efforts by the Star Blizzard Defendants to continue to operate the Star Blizzard spear phishing operation. 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 the instant case, where notice would render the requested relief

ineffective. *See, e.g.*, *Council on Am.-Islamic Relations v. Gaubatz*, 667 F. Supp. 2d 67, 73–74 (D.D.C. 2009) (granting *ex parte* TRO); *In re BAE Sys. PLC Derivative Litig.*, No. 07-1646, 2008 WL 458575, at *1 (D.D.C. Feb. 5, 2008) (granting *ex parte* TRO to enjoin party from selling U.S.-based assets allegedly acquired with bribe payments); *AT&T Broadband v. Tech Commc'ns, Inc.*, 381 F.3d 1309, 1319-1320 (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 was given); *Allscripts Misys, LLC v. Am. Dig. Networks, LLC*, 1:10-cv-00111, 2010 U.S. Dist. LEXIS 4450, at *2 (D. Md. Jan. 20, 2010) (granting *ex parte* TRO where "Defendant may dissipate the funds and/or take action to render it difficult to recover funds"); *Crosby v. Petromed, Inc.*, No. CV-09-5055, 2009 WL 2432322, at *2 (E.D. Wash. Aug. 6, 2009) (granting *ex parte* TRO as "notice to Defendants of this TRO request could result in further injury or damage to Plaintiffs...."); *Little Tor Auto Ctr. v. Exxon Co., U.S.A.*, 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"). For the same reason that the Court found that *ex parte* relief was appropriate in connection with the TRO, it is appropriate here. Dkt. No. 12 (TRO) at 6. If the Star Blizzard Defendants are made aware of Plaintiffs supplemental efforts to take down the new domains and curtail the Star Blizzard Defendants' rebuilding efforts, the Star Blizzard Defendants will take steps to relocate their operations to prevent yet another devastating blow to their spear phishing operation.

Immediately upon execution of the Supplemental Preliminary Injunction and disablement of the additional domains addressed in the attached proposed order, Plaintiffs will provide robust notice to the Star Blizzard Defendants. *Id.* at 10-11. Plaintiffs will provide the Star Blizzard Defendants the documents associated with this motion and the Court's order, by sending them to

all of the Star Blizzard Defendants' contact information associated with the subject domains, thus providing notice and an opportunity to appear and contest the requested relief, if the Star Blizzard Defendants so choose. *Id.*

III. CONCLUSION

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

Dated: November 5, 2024

/s/ *Jeffrey L. Poston*
Jeffrey L. Poston (DC Bar No. 426178)
Garylene Ana Joji D. Javier (*pro hac vice*)
JPoston@crowell.com
GJavier@crowell.com
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington, DC 20004

Anna Z. Saber (*pro hac vice*)
ASaber@crowell.com
CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111

Attorneys for Plaintiffs Microsoft Corporation and NGO-ISAC