

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

MICROSOFT CORPORATION, a
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-2,
Controlling A Computer Network and
Thereby Injuring Plaintiff and Its Customers,

Defendants.

Civil Action No: 1:21-cv-01346

**FILED UNDER SEAL PURSUANT TO
LOCAL RULE 5.1**

**BRIEF IN SUPPORT OF MICROSOFT'S *EX PARTE* MOTION TO SUPPLEMENT
PRELIMINARY INJUNCTION ORDER**

Plaintiff Microsoft Corporation ("Microsoft") seeks an *Ex Parte* Supplemental Preliminary Injunction Order to address Defendants' continuing efforts to rebuild Nickel's command and control infrastructure and continue their illegal activities in open defiance of this Court's Preliminary Injunction Order. Microsoft expresses its appreciation for the continued attention of the Court to this ongoing cybersecurity matter.

Microsoft incorporates by reference herein the arguments and evidence set forth in its Brief in Support Of Microsoft's Application for an *Ex Parte* Temporary Restraining Order and Order To Show Cause Re Preliminary Injunction ("TRO Application"). Dkt. No. 6. As discussed in Microsoft's TRO Application, the domains used in Nickel's command and control infrastructure are critical to Nickel's operation. The most effective way to disable Nickel's operation is to disable the Internet domains used by John Does 1-2 ("Defendants").

I. BACKGROUND

On December 2, 2021, the Court granted an Emergency *Ex Parte* Temporary Restraining Order (“TRO”) tailored to halt the illegal activities and the growth of the Nickel operation. Dkt. 4. Through the Nickel operation, Defendants infiltrate the online accounts of Microsoft’s customers, the hijacking of the Microsoft’s Windows operating system and other Microsoft software on infected computers, and theft of users’ credentials and information. Defendants cause great harm to Microsoft by damaging the products that Microsoft licenses to its customers. Further, by exploiting Microsoft’s famous and highly-regarded trademarks, products, and services to disguise and further its criminal conduct, Defendants cause Microsoft irreparable reputational and other harms for which no monetary recourse is available.

As explained in Microsoft’s 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. 6. These domains are used both to break into computers and networks of the organizations that Nickel targets, control the reconnaissance of those networks, and ultimately, exfiltrate sensitive information from them. On December 7, 2021, to disable this command and control infrastructure, this Court ordered that these Nickel-controlled Internet domains, listed in the Appendix A filed on December 2, 2021, be redirected to secure Microsoft servers when it granted a Preliminary Injunction. Dkt. No. 24.

However, Defendants 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. Indeed, this probability was foreseen by the Court in issuing its TRO. And as foreseen, following the execution of the TRO and Preliminary Injunction, Defendants openly defied this Court and started to rebuild their command and control infrastructure by adding new Internet

domains to Nickel's command and control infrastructure in order to target new accounts and exposing potential new victims to Nickel. Further, the domain creation and webhosting patterns exhibit consistencies with the domain creation and webhosting patterns seen with prior known domains created by the Nickel Defendants. Declaration of Christopher Coy in Support of Motion to Supplement Preliminary Injunction ("Coy Decl.") ¶ 5.

Consequently, Microsoft is asking the Court to allow it to redirect six new Nickel-controlled domains to Microsoft secure servers. This will disrupt Defendants' recent illegal activity. A list of the new domains used by Defendants is provided in the **Appendix A** to the Proposed Order filed concurrently with this brief.

II. ARGUMENT

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

Microsoft seeks to 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 Microsoft 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 Microsoft Corp. v. John Does 1-8*, Case No. 1:14-cv-00811-LOG-TCB (E.D. Va. 2014) (O'Grady, J.) at Dkt. No. 32 (disabling the "Shylock" botnet).

Here, absent the requested relief, irreparable harm will continue to Microsoft and its customers, for the reasons detailed in Microsoft's prior submissions. Microsoft is 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 Microsoft's previous motion for TRO and Preliminary Injunction. Coy Decl. ¶¶ 7, 13. For example, the domains "mfagcesk[.]com," "sanocraftics[.]com,"

“wmdelmys[.]com,” and “bildspro[.]com” were observed disseminating Nickel malware to unsuspecting victims. The domains “futuragore[.]com” and glf.co[.]com” were identified because domain creation and webhosting patterns exhibit consistencies with the domain creation and webhosting patterns seen with prior known domains created by the Nickel Defendants. Thus, pursuant to Federal Rule of Civil Procedure 65, disabling the additional six domains at issue is necessary to prevent harm to Microsoft and its 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. Declaration of Christopher Coy in Support of Motion for Temporary Restraining Order and Preliminary Injunction (“Coy TRO Decl.”) ¶¶ 45-48. Thus, providing notice of the requested *ex parte* relief will undoubtedly facilitate efforts by Defendants to continue to operate Nickel. 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”).

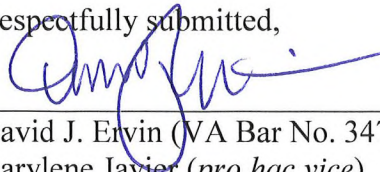
As before in this matter, immediately upon execution of the Supplemental Preliminary Injunction and disablement of the additional domains addressed in the attached proposed order, Microsoft will provide robust notice to the defendants. Microsoft will provide defendants the documents associated with this 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 Coy Declaration submitted with the prior Application for TRO, and based on the evidence submitted with the Application for TRO and Preliminary Injunction, Microsoft respectfully requests that the Court grant Microsoft’s Motion to Supplement the Preliminary Injunction Order.

Dated: February 28, 2022

Respectfully submitted,



David J. Ervin (VA Bar No. 34719)

Garylene Javier (*pro hac vice*)

CROWELL & MORING LLP

1001 Pennsylvania Avenue NW

Washington DC 20004-2595

Tel: (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

Tel: (415) 986-2800

Fax: (415) 986-2827

gramsey@crowell.com

kghaffari@crowell.com

Attorneys for Plaintiff Microsoft Corporation