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: 1:16-cv-00993 (GBL/TCB) **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5**

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 Defendant's continuing efforts to rebuild Strontium'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 cyber-security 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 (Dkt. No. 12) ("Microsoft's TRO Application") and Brief In Support of Microsoft's Motion to Amend Preliminary Injunction Order (Dkt. No. 37). As discussed in Microsoft's TRO Application, the domains used in Strontium's command and control infrastructure are critical to Strontium's operation. The most effective way to disable

Strontium's operation is to disable the Internet domains used by John Does 1-2 ("Defendants").

I. BACKGROUND

On August 5, 2016, the Court granted an Emergency *Ex Parte* Temporary Restraining Order ("TRO") tailored to halt the illegal activities and the growth of the Strontium operation. Through the Strontium operation, Defendants lure victims into clicking on links embedded in personalized e-mails thereby compromising their computers, computer networks and accounts hosted on Microsoft's servers, all with the goal of stealing the victims' sensitive data. 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 using an online command and control infrastructure consisting of a set of websites and domains. Dkt. No. 12, pp. 5-12. These domains are used both to break into computers and networks of the organizations that Strontium targets, control the reconnaissance of those networks, and, ultimately, exfiltrate sensitive information from them. To disable this command and control infrastructure, this Court ordered that these Strontium-controlled Internet domains, listed in the Appendix A to the TRO, be redirected to secure Microsoft sinkhole servers. On August 12, 2016, the Court converted the TRO into a Preliminary Injunction. Dkt. No. 33.

Executing the Court's Temporary Restraining Order and Preliminary Injunction Order, Microsoft cut communications between Defendants' existing command and control infrastructure and the victim computers and networks that Defendants had attacked and from which Defendants had been stealing information. Declaration of Jason L. Norton In Support Of Microsoft's Motion To Supplement Preliminary Injunction Order ("Norton Decl.") ¶¶ 4, 5. This effectively stymied Defendants' efforts to exploit the computers and networks they had targeted or already broken into. Indeed, since the execution of the TRO, Microsoft disrupted attacks on at least 122 victims targeted by Defendants. *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. 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 associated with Microsoft trademarks to Strontium's command and control infrastructure. *Id.* ¶¶ 6-7. Consequently, on August 29, 2016, the Court allowed Microsoft to redirect 18 new Strontium-controlled domains to Microsoft secure servers. Dkt. No. 39. Again, while this disrupted Defendants activity for a time, recent evidence shows that Defendants are again rebuilding Strontium's command and control infrastructure by adding new domains. A list of the new domains used by Defendants is provided in the Second Amended Appendix A to the Proposed Order filed concurrently with this brief. The domains added to Appendix A are contained under the heading "NOVEMBER 9, 2016 AMENDMENT."

II. ARGUMENT

A. There Is Good Cause to Amend Appendix A To The Preliminary Injunction Order Ex Parte

Microsoft seeks to amend the Preliminary Injunction Order by replacing the August 26, 2016 Amended Appendix A (Dkt. No. 29) with the Second Amended Appendix A to the Proposed Order submitted with this motion. 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. l:14-cv-00811-LOG-TCB (E.D. Va. 2014) (O'Grady, J.) at Dkt. No. 32 (disabling the "Shylock" botnet).

With respect to Amending Appendix A to the Preliminary Injunction Order, *ex parte* relief is essential. If notice is given prior to issuance of a the Supplemental Preliminary Injunctive Order, 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. Norton Decl. ¶¶ 6-7. Thus, providing notice of the requested *ex parte* relief will undoubtedly facilitate efforts by the Defendants to continue to operate Strontium. 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., AllscriptsMisys, LLC v. Am. Digital Networks, LLC,* 1:10-cv-00111, 2010 U.S. Dist. LEXIS 4450, at *2 (D. Md. Jan. 20, 2010) (granting an *ex parte* TRO where "Defendant may dissipate the funds and/or take action to render it difficult to recover funds …."); *Crosby v. Petromed, Inc*., 2:09-cv-05055, 2009 U.S. Dist. LEXIS 73419, at *5 (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....").

Thus, pursuant to Federal Rule of Civil Procedure 65, disabling that infrastructure is necessary to prevent harm to Microsoft and its customers.

B. An Ongoing Process Is Needed To Efficiently And Effectively Curtail Defendants' Efforts To Rebuild Strontium's Command And Control Infrastructure

Microsoft seeks to supplement the Preliminary Injunction Order, by establishing a streamlined procedure, assisted by a court-appointed monitor, to respond to new malicious domains registered by Defendants in violation of the injunction, as set forth more fully in the Proposed Order submitted with this motion.

Defendants are persistent in their activities and are likely to attempt to maintain, rebuild, and even grow, their capabilities again and again. Microsoft will, as it has up until now, monitor Defendants' activities, identify new Strontium command and control domains associated with Microsoft trademarks or brands ("Strontium Domains") as they are activated, and will seek

additional supplemental relief from the Court. Consequently, Microsoft and the Court face the prospect that enforcing the Court's order will require multiple ongoing rounds of amendments to the list of command and control domains subject to the Court's preliminary injunction order and multiple new proceedings. Failing this sustained effort, Defendants will continue their malicious and illegal activities, causing irreparable injury to Microsoft, its customers and the public. Norton Decl. ¶ 17.

However, Microsoft acknowledges the burden that such a sustained effort will place on the Court. Microsoft therefore respectfully submits that a streamlined procedure is advisable to efficiently and effectively supplement the list of domains subject to the Court's order as soon as Defendants activate the new domains. In brief, Microsoft recommends that the Court appoint a Court Monitor, pursuant to Federal Rule of Civil Procedure 53, to manage this process and relieve the burden on the Court. The availability of a Court Monitor to oversee this process also increases the effectiveness of the Court's prior injunctive orders, as it will enable more prompt, continuous response to Defendants' continued violation of the orders. The Court Monitor will make determinations on any disputes between Microsoft, any Defendant, registry or other third party, regarding disabling of Strontium Domains set forth in the Proposed Order. The Court Monitor will further determine (based on evidence submitted by Microsoft) whether additional particular domains are in fact being used by Defendants as part of Strontium and may order that such new domains be added to the list of domains subject to the Court's injunctive orders. The Court Monitor will also monitor Defendants' compliance with the Court's orders.

Under Federal Rule of Civil Procedure 53(a)(1)(C), a court may appoint a court monitor to "address pretrial and posttrial matters that cannot be effectively and timely addressed by an available district judge or magistrate judge of the district." A court monitor is necessary here because it will impose an undue burden on the court's limited time and resources to rule on what are expected to be continuous and potentially frequent motions to amend the Preliminary Injunction Order every time that Defendants register and use new Strontium Domains leveraging Microsoft trademarks. This is especially the case considering the ease and speed with which

Defendants are currently registering Microsoft-related domains to continue their attacks. Further, the ability of a court monitor to make determinations on such matters will increase the effectiveness of the Court's existing injunctions and permit enforcement of Defendants' compliance on an ongoing basis. Courts have frequently made use of court-appointed monitors and other masters in cases such as this one, where ongoing compliance with the court's orders is at issue and supervision would be too time-consuming or difficult for the court to undertake without assistance. *See e.g.*, *Ohio Valley Envtl. Coal. v. Fola Coal Co., LLC*, No. 2:13-21588, 2016 U.S. Dist. LEXIS 73904, at *50 (S.D. W. Va. June 7, 2016) ("Appointing a special master is proper in this case because the proposed injunctive relief includes complex analysis and implementation of environmental engineering plans and monitoring to correct [defendant's] violations."); *Sledge v. J.P. Stevens & Co., Civil No. 1201., 1976 U.S. Dist. LEXIS 16422, at *29 (E.D.N.C. Feb. 27, 1976)* (Appointing a Special Master to administer the Court's Decree and to hear and determine instances of possible non-compliance); *Schaefer Fan Co. v. J & D Mfg., Inc.*, 265 F.3d 1282 (Fed. Cir. 2001) (Appointing special master to resolve disputes and issue decisions regarding compliance with settlement agreement); *Evans v. Fenty*, 701 F. Supp. 2d 126, 129 (D.D.C. 2010) (Special Masters assisted court by making findings and recommendations that addressed the status of defendants' compliance and available options for curing the identified deficiencies); *see also* 18 U.S.C. § 1836(b)(2)(D) (providing that special masters may be appointed to locate and isolate trade secret information from other property).

As the first step in the streamlined process in the Proposed Order, Microsoft will monitor Defendants' activities and will identify new Microsoft related Strontium Domains as Defendants activate them. Making an accurate identification is crucial, and Microsoft will base its conclusions on a set of criteria developed over the course of its lengthy investigation into Defendants and Strontium. Norton Decl. ¶ 8-15. The following are factors Microsoft considers within its framework.

1. ***Presence of Distinctive Malware***: Defendants typically use a relatively small set of distinctive malware that can be distinguished from other types of malware.

Id. ¶ 9. The specific types of malware known to be used by Defendants is listed in Exhibit A to Jason Norton's Declaration. If the malware used in a new attack matches or is a similar variant of the distinctive malware used by the Defendants in past attacks, it indicates that the actors behind the new attack are the Defendants. *Id.* Because Strontium malware is reasonably distinctive, domains that are used to deliver the Strontium malware to targeted victims or communicate with the Strontium malware already installed on victims' networks are strongly implicated as Strontium domains. *Id.* The presence of this distinctive malware therefore serves as a reliable indicator that Defendants are using the Internet domain at issue. *Id.*

2. ***Pattern in Domain Registration***: If the registration information associated with a newly identified Internet domain closely matches the pattern associated with the domains registered by the Defendants in the past, it is a strong indicator that the Defendants are behind the registration of the new domain. *Id.* ¶ 11. Microsoft has identified patterns in the registration information provided by Defendants when registering the domains used in their illegal activities. *Id.* Microsoft considers such things as the e-mail address and phone number provided by the registrant, the hosting service designated, the name servers used, the IP address(es) and other technical details associated with the domain. *Id.* Exemplary registration information associated with Internet domains registered by Defendants in the past is included in Appendix A to the Proposed Order filed concurrently with this brief.
3. ***Tactics Used During a New Attack***: Where the tactics used in a new attack match the tactics favored by Strontium Defendants in past attacks, it is an indication that the Defendants are behind the new attack. *Id.* ¶ 12. For example, Strontium Defendants often send phishing e-mails to victims in which the e-mail purports to be a notification from Microsoft regarding an unauthorized access to

the recipients' Microsoft account, and requesting that she or he reset the account credentials. *Id.* If the victim clicks on the embedded "Change Password" button in the phishing e-mail, the victim will be connected to a Strontium-controlled website which will attempt to induce the victim to enter his account credentials. *Id.* Other tactics favored by the Strontium Defendants include remote code execution through browser drive-by, remote code execution through malicious attachments, privilege escalation or sandbox escape, security feature bypass, social engineering based attack and/or bootstrapped add-on. *Id.*

4. ***Specific Targeted Victims***: The Strontium Defendants tend to target a particular type of victim and attempt to steal particular types of information. *Id.* ¶ 13. Therefore, Microsoft can use information about the intended victim to help determine whether or not Defendants are involved in the new attack. *Id.* For example, Strontium continues to target charities, Non-Government Organizations (NGOs), diplomatic institutions, political operations, and military organizations in the United States, Europe, and Asia. *Id.* Where an Internet domain is associated with an attack on these particular types of targets, it is a factor that is consistent with the known activity and objectives of the Defendants.
5. ***Use of Microsoft Marks and Brands or Confusingly Similar Variants***: The use of Microsoft trademarks and brand names or slight misspellings or variants of those trademarks or brand names in the domain name, alone or in combination with other terms, is an indicator that the domain is associated with Strontium. The Strontium Defendants have used Microsoft trademarked brands (e.g., microsoftstoreservice.com" and "login outlook.com") or slight misspellings of those brands (e.g., "wind0ws.kz" and "windous.kz") in the names of the domains that they register for their illegal activity. *Id.* ¶¶ 7, 14. Defendants use this technique to disguise the illegal nature of their conduct from the intended target. *Id.* ¶ 14. By studying the ways in which the Defendants have incorporated

Microsoft's trademarks and brand names into domain names that Defendants have used in the past, Microsoft is able to anticipate the domain names Defendants are most likely to use in the future. *Id.* ¶ 16. Microsoft generated a list of the domain names Defendants are most likely to use going forward. This list is attached as Appendix B to the Proposed Order filed concurrently with this brief. *Id.*

Under Microsoft's proposal, when Microsoft determines that Defendants have activated a new Microsoft related Strontium Domain, the disposition of that domain can follow one of two paths. First, with respect to domains listed in Appendix B, Microsoft shall serve written notice of such determination on the relevant domain registries. Upon receipt of such written notice, the domain registries will be required to promptly implement the Court's order, including by redirecting the domains to Microsoft's servers. If the domain registries dispute Microsoft's determinations, or if Defendants or any third party dispute action taken by domain registries or Microsoft's determinations pursuant to this Order, the domain registries, Defendants or any third parties may submit written objections to the Court Monitor for resolution by the Court Monitor, subject to the right to judicial review. In the course of deciding any objections submitted by registries, Defendants or third parties, the Court Monitor shall take and hear evidence and shall make determinations and issue orders whether domains are Strontium Domains.

Second, with respect to (a) domains not listed in Appendix B, but which are otherwise alleged to meet the criteria to constitute Microsoft related Strontium Domains, and (b) domains that are alleged to be Strontium Domains based on new criteria, Microsoft shall submit a written motion to the Court Monitor seeking a declaration that such domains are Strontium Domains. The Court Monitor shall take and hear evidence and shall make determinations and issue orders whether domains are Strontium Domains, again, subject to the right to judicial review.

Microsoft believes this process will reduce the burden on the Court, better ensure enforcement of the Court's orders, provide for efficient reaction against Defendants as they attempt to activate new domains for illegal ends, and provide an adequate mechanism for registries, third-parties, or Defendants to challenge the substance and process concerning

enforcement of the injunction. Thus, the appointment of a court monitor in this case is appropriate under Federal Rule of Civil Procedure 53(a)(1)(C).

If the Court is amenable to appointment of a Court Monitor to oversee ongoing enforcement of the injunction, Microsoft respectfully requests the Court's recommendations concerning potential candidates for this role. In order to assist the Court, Microsoft proposes Hon. Faith Hochberg (Ret.) to serve as the Court Monitor. Judge Hochberg has relevant legal and technical expertise and has served in the capacity as a neutral special master in prior matters. Any Court Monitor must establish that there are no conflicts of interest and provide an affidavit "disclosing whether there is any ground for disqualification under 28 U.S.C. § 455." A declaration of the foregoing candidate for the role of Court Monitor, including current curriculum vitae, is submitted concurrently with this motion, for the Court's consideration.

III. CONCLUSION

For the reasons set forth in this brief, the Norton Declaration submitted with this brief and based on the evidence submitted with the TRO Application, Microsoft respectfully requests that the Court grant Microsoft's Motion To Supplement Preliminary Injunction Order.

Dated: November 14, 2016 Respectfully submitted,

ORRICK, HERRINGTON & SUTCLIFFE LLP

/s/ Sten Jensen

STEN JENSEN
Va. State Bar No. 38197
Attorney for Plaintiff Microsoft Corp.
ORRICK, HERRINGTON SUTCLIFFE LLP
Columbia Center
1152 15th Street, N.W.
Washington, D.C. 20005-1706
Telephone: (202) 339-8400
Fax: (202)-339-8500
sjensen@orrick.com

Of counsel:

GABRIEL M. RAMSEY (admitted *pro hac vice*)
Attorney for Plaintiff Microsoft Corp.
ORRICK, HERRINGTON & SUTCLIFFE LLP
405 Howard Street
San Francisco, CA 94105-2669
Telephone: (415) 773-5700
Fax: (415) 773-5759
gramsey@orrick.com

JEFFREY L. COX (admitted *pro hac vice*)
Attorney for Plaintiff Microsoft Corp.
ORRICK, HERRINGTON & SUTCLIFFE LLP
701 Suite Seattle, WA 98104-7097
Telephone: (206) 839-4300
Fax: (206) 839-4301
jcox@orrick.com

RICHARD DOMINGUES BOSCOVICH
CRAIG LEE MOSES
Attorneys for Plaintiff Microsoft Corp.
MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052-6399
Telephone: (425) 704-0867
Fax: (425) 936-7329
rbosco@microsoft.com
crmoses@microsoft.com