IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

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: 1:19-cv-00716-ABJ **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5.1**

[PROPOSED] SECOND SUPPLEMENTAL INJUNCTION ORDER

The Court, having considered the pleadings and declaration in support of Microsoft Corporation's ("Microsoft") Motion for Second Supplemental Preliminary Injunction Order, hereby orders that (i) the terms of the Preliminary Injunction Order ("Preliminary Injunction Order"), Dkt. 18, shall apply to the additional domains set forth in the **Appendix A** to this order established by Defendants in violation of this court's order and (ii) appoint a Court Monitor, pursuant to Federal Rule of Civil Procedure 53, to manage this process and relieve the burden on the Court.

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, memorandum, and all other pleadings and papers relevant to Microsoft's Motion for Second Supplemental Preliminary Injunction Order and Microsoft's original motion for Temporary Restraining Order and Preliminary Injunction, the Court hereby makes the following findings of fact and conclusions of law:

I. The Defendants were served with notice of the Preliminary Injunction.

II. After receiving notice of the Preliminary Injunction, the Defendants have continued to engage in the conduct enjoined by the Preliminary Injunction Order, and therefore continue to violate the Preliminary Injunction Order. In particular, Defendants have intentionally and without authorization, continued and attempted to access and send malicious software, code, and instructions to protected computers, operating systems, and networks of Microsoft and its customers, attacking such computers, systems and networks, and exfiltrating information from those computers, systems and networks, using new domains.

III. There is good cause to believe that Defendants are likely to continue the foregoing conduct and to engage in the illegal conduct and purposes enjoined by the Preliminary Injunction Order, unless further relief is ordered to expeditiously prevent Defendants from maintaining the registration of domains for such prohibited and unlawful purposes.

IV. There is good cause to believe that, unless further relief is ordered to expeditiously prevent Defendants from maintaining the registration of domains for purposes enjoined by the Preliminary Injunction Order, immediate and irreparable harm will result to Microsoft, Microsoft's customers and to the public, from the Defendants' ongoing violations.

V. Therefore, in accordance with Fed. R. Civ. P. 65(b), 15 U.S.C. § 1116(a) and 28 U.S.C. § 1651(a) and the Court's inherent equitable authority, good cause and the interests of justice require that this Order be Granted.

SECOND SUPPLEMENTAL PRELIMINARY INJUNCTION

IT IS THEREFORE ORDERED that, the terms of the Preliminary Injunction Order shall be supplemented and shall be enforced against Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants, as follows:

1. With respect to any currently registered Internet domains set forth in **Appendix**

A, the domain registries shall take the following actions:

A. Within five (5) business days of receipt of this Order, shall unlock and change the registrar of record for the domain to MarkMonitor or such other registrar specified by Microsoft. To the extent the registrar of record does not assist in changing the registrar of record for the domain under its control, the domain registry for the domain, or its administrators, including backend registry operators or administrators, within five (5) business days of receipt of this Order, shall change, or assist in changing, the registrar of record for the domain to MarkMonitor or such other registrar specified by Microsoft. The purpose of this paragraph is to ensure that Microsoft has control over the hosting and administration of the domain in its registrar account at MarkMonitor or such other registrar specified by Microsoft. Microsoft shall provide to the domain registry or registrar of record any requested registrar information or account details necessary to effectuate the foregoing.

B. The domain shall be made active and shall resolve in the manner set forth in this order, or as otherwise specified by Microsoft, upon taking control of the domain;

C. The domain shall be redirected to secure servers by changing the authoritative name servers to NS151.microsoftinternetsafety.net and NS152.microsoftinternetsafety.net and, as may be necessary, the IP addresses associated with name servers or taking other reasonable steps to work with Microsoft to ensure the redirection of the domain and to ensure that Defendants cannot use it to make unauthorized access to computers, infect computers, compromise computers and computer networks, monitor the owners and users of computers and computer networks, steal information from them or engage in any other activities prohibited by the Injunction;

D. The WHOIS registrant, administrative, billing and technical contact and

identifying information should be the following, or other information as may be specified by Microsoft:

Domain Administrator
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
United States
Phone: +1.4258828080
Facsimile: +1.4259367329
domains@microsoft.com

E. Prevent transfer, modification or deletion of the domain by Defendants and prevent transfer or control of the domain to the account of any party other than Microsoft;

F. Take all steps required to propagate to the foregoing changes through the Domain Name System ("DNS"), including domain registrars.

IT IS FURTHER ORDERED that "Phosphorus Domains" are domains which are determined to meet the following two criteria:

Criteria 1: The domains are used by the Defendants to break into computers and networks of the organizations that Phosphorus targets, or control the reconnaissance of those networks, or, ultimately, exfiltrate sensitive information from them, or are otherwise used by the Defendants to carry out the activities and purposes prohibited by the Preliminary Injunction. A domain is determined to be a Phosphorus Domain by comparing the activities and patterns associated with that domain with known confirmed Phosphorus Domains. The following factors concerning the domain will be used in this analysis:

Delivers malicious software, code, commands, exploits and/or "backdoor" functionality previously associated with Phosphorus, including but not limited to: Stealer malware, or similar code or functionality deployed in a manner previously associated with Phosphorus.	Associated with remote code execution through browser drive-by or malicious attachment, privilege escalation or sandbox escape, security feature bypass, social engineering based attack and/or bootstrapped add-on, escalation of privileges, DLL file backdoor, credential stealing functionality, SSL tunnel, and/or functionality to deliver code or functions to "air gapped" USB devices, deployed in a manner

	previously associated with Phosphorus or similar code or functionality.
Domain registration information	Use of cryptocurrency to purchase services
Name servers	Start of Authority (SOA) records
Resolves to IP of past Phosphorus domain, command and control server or similar infrastructure	Resolves to IP used in past Phosphorus malware delivery or credential harvesting domains or credential harvesting domains
Used to deceive, target, obtain information from, and/or communicate commands or code to recipients, persons, institutions or networks previously targeted by Phosphorus.	Used to deceive, target, obtain information from, and/or communicate commands or code to recipients that may possess or be able to provide sensitive information or trade secrets of persons, entities or networks related to the defense, critical infrastructure or high technology sectors, journalists, political advisors or organizations, government bodies, diplomatic institutions, religious organizations, universities, and/or military forces and installations.
SSL Cert Issuer_DN	SSL Cert Subject_DN
Host	Registrar
Domains similar to previously used domains	Victims being targeted similar to past targets

Criteria 2: The domains (a) use and infringe Microsoft's trademarks, trade names or service marks or confusingly similar variants, or (b) use any false or deceptive designation, representation or description, which would damage or injure Microsoft or give Defendants an unfair competitive advantage or result in deception of consumers, or (c) suggest in any way that Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Microsoft, or pass off Defendants' activities, products or services as Microsoft's. Such trademarks and brands shall include, but are not limited to the following trademarks, brands and/or confusingly similar variants: While Defendants may use any Microsoft marks, brands or confusingly similar indicators, Defendants have already exploited or are likely to exploit the following: "365," "Azure," "Bing," "Excel," "Exchange," "Healthvault," "Hotmail," "LinkedIn," "Live," "Messenger," "Microsoft," "Minecraft," "MSDN," "MSFT," "MS," "MSN," ".NET," O365," "Office," "OneDrive," "Outlook," "OWA," "Passport," "PowerPoint,"

"SharePoint," "Skype," "Surface," "Visio," "Win," "Windows," and "Xbox." Also, Criteria 2 is met where defendants use generalized versions of terms that are suggestive of Microsoft's services, but do not specifically use a trademark.

IT IS FURTHER ORDERED that the following processes shall be used to determine whether a domain is a Phosphorus Domain and to determine the disposition of such domains. With respect to domains alleged to meet the criteria to constitute Phosphorus Domains, and domains that are alleged to be Phosphorus Domains based on new criteria not listed in this Order, Microsoft shall submit a written motion to the Court Monitor seeking a declaration that such domains are Phosphorus Domains. The Court Monitor shall take and hear evidence and shall make determinations and issue orders whether domains are Phosphorus Domains, as set forth further below.

IT IS FURTHER ORDERED that, pursuant to Federal Rule of Civil Procedure 53(a)(l)(C) and the court's inherent equitable powers, Hon. Faith Hochberg (Ret..) is appointed to serve as Court Monitor in order to make determinations on disputes regarding whether particular domains are Phosphorus Domains, to make determinations and orders regarding whether particular domains are Phosphorus Domains, and to monitor Defendants' compliance with the Preliminary Injunction. Prior to being appointed, the Court Monitor must file an affidavit "disclosing whether there is any ground for disqualification under 28 U.S.C. § 455." Fed. R. Civ. P. 53(b)(3); *see also* Fed. R. Civ. P. 53(a)(2) (discussing grounds for disqualification). Filed concurrently with this Order is the affidavit submitted to the court by the Court Monitor. The following sets forth the terms of the appointment of the Court Monitor:

1. **Duties:** The duties of the Court Monitor shall include the following:

    A. Carrying out all responsibilities and tasks specifically assigned to the

Court Monitor in this Order;

B. Resolving objections submitted by domain registries, Defendants or other third parties, to Microsoft's determinations that domains constitute Phosphorus Domains and, with respect to motions submitted by Microsoft that particular domains constitute Phosphorus Domains, making determinations whether such domains are or are not Phosphorus Domains;

C. Otherwise facilitating the Parties' or third parties' resolution of disputes concerning compliance with obligations under this Order or any orders issued by the Court Monitor, and recommending appropriate action by the court in the event an issue cannot be resolved by the Parties or third parties with the Court Monitor's assistance;

D. Investigating matters related to the Court Monitor's duties, and enforcing orders related to the matters set forth in this Order

E. Monitoring and reporting on Defendants' compliance with their obligations under the Preliminary Injunction and this Order;

F. The Court Monitor shall have all authority provided under Federal Rule of Civil Procedure 53(c).

2. Orders Regarding Phosphorus Domains: The Court Monitor shall resolve objections and shall make determinations and issue orders whether domains are Phosphorus Domains, pursuant to the terms set forth in the Preliminary Injunction, this Order and pursuant to the following process:

A. Upon receipt of a written objection from any domain registries, Defendants or any other third parties contesting any determinations by Microsoft that particular domains constitute Phosphorus Domains, or upon receipt of a written motion from Microsoft for a finding that particular domains constitute Phosphorus Domains, the Court Monitor shall take

and hear evidence whether a domain is a Phosphorus Domain, pursuant to the standards set forth in Rule 65 of the Federal Rules of Civil Procedure. Any party opposing such objection or motion shall submit to the Court Monitor and serve on all parties an opposition or other response within twenty four (24) hours of receipt of service of the objection or motion. The Court Monitor shall issue a written ruling on the objection or motion no later than two (2) days after receipt of the opposition or other response. Any party may seek and the Court Monitor may order provisional relief, including redirection of domains or other temporary disposition of domains, while any objection or motion is pending. A form of order which may be used by the Special Master is attached as **Appendix B**.

B. It is the express purpose of this order to afford prompt and efficient relief and disposition of Phosphorus Domains. Accordingly, in furtherance of this purpose, all objections, motions and responses shall be embodied and communicated between the Court Monitor, parties and third parties in electronic form, by electronic mail or such other means as may be reasonably specified by the Court Monitor. Also in furtherance of this purpose, hearings shall be telephonic or in another expedited form as may be reasonably specified by the Court Monitor.

C. The Court Monitor's determinations regarding any objection or any motion shall be embodied in a written order, which shall be served on all Parties and relevant third parties (including domain registries and/or registrars).

D. The Court Monitor is authorized to order the Parties and third parties to comply with such orders (pursuant to 28 U.S.C. § 165l(a)), subject to the Parties' and third parties' right to judicial review, as set forth herein.

E. If no Party or third party objects to the Court Monitor's orders and

determinations pursuant to the judicial review provisions herein, then the Court Monitor's orders and determinations need not be filed on the docket. However, at the time the Court Monitor submits his or her periodic reports to the court, as set forth below, the Monitor shall separately list in summary form his or her uncontested orders and determinations.

3. Judicial Review: Judicial review of the Court Monitor's orders, reports or recommendations, shall be carried out as follows:

A. If any Party or third party desires to object to any order or decision made by the Court Monitor, the Party shall notify the Court Monitor within one business day of receipt of service of the order or decision, and thereupon the Court Monitor shall promptly file on the court's docket the written order setting forth the Monitor's decision or conditions pursuant to Federal Rule of Civil Procedure 53(d). The Party or third party shall then object to the Court Monitor's order in the manner prescribed in this Order.

B. The Parties and third parties may file objections to, or a motion to adopt or modify, the Court Monitor's order, report, or recommendations no later than 10 calendar days after the order is filed on the docket. The court will review these objections under the standards set forth in Federal Rule of Civil Procedure 53(f).

C. Any party may seek and the Court may order provisional relief, including redirection of domains or other temporary disposition of domains, while any objection or motion is pending.

D. The orders, reports and recommendations of the Court Monitor may be introduced as evidence in accordance with the Federal Rules of Evidence.

E. Before a Party or third party seeks relief from the court for alleged noncompliance with any court order that is based upon the Court Monitor's report or

recommendations, the Party or third party shall: (i) promptly notify the other Parties or third party and the Court Monitor in writing; (ii) permit the Party or third party who is alleged to be in noncompliance five business days to provide the Court Monitor and the other parties with a written response to the notice, which either shows that the party is in compliance, or proposes a plan to cure the noncompliance; and (iii) provide the Court Monitor and parties an opportunity to resolve the issue through discussion. The Court Monitor shall attempt to resolve any such issue of noncompliance as expeditiously as possible.

4. Recordkeeping: The Court Monitor shall maintain records of, but need not file those orders, reports and recommendations which are uncontested by the Parties or third parties and for which judicial review is not sought. The Court Monitor shall file on the court's docket all written orders, reports and recommendations for which judicial review is sought, along with any evidence that the Court Monitor believes will assist the court in reviewing the order, report, or recommendation. The Court Monitor shall preserve any documents the Monitor receives from the Parties.

5. Periodic Reporting: The Court Monitor shall provide periodic reports to the court and to the Parties concerning the status of Defendants' compliance with this Order and other orders of the court or the Court Monitor, including progress, any barriers to compliance, and potential areas of noncompliance. The periodic reports shall also include a summary of all uncontested orders and determinations and a listing of ex parte communications. The Court Monitor shall file a report with the court under this provision at least once every 120 days.

6. Access to Information: The Court Monitor shall have access to individuals and non-privileged information, documents, and materials under the control of the Parties or third parties that the Monitor requires to perform his or her duties under this Order, subject to the

terms of judicial review set forth herein. The Court Monitor may communicate with a Party's or a third party's counsel or staff on an *ex parte* basis if reasonably necessary to carry out the Court Monitor's duties under this Order. The Court Monitor may communicate with the court on an *ex parte* basis concerning non-substantive matters such as scheduling or the status of the Court Monitor's work. The Court Monitor may communicate with the court on an *ex parte* basis concerning substantive matters with 24 hours written notice to the Parties and any relevant third party. The Court Monitor shall document all *ex parte* oral communications with a Party's or third party's counsel or staff in a written memorandum to file summarizing the substance of the communications, the participants to the communication, the date and time of the communication and the purpose of the *ex parte* communication. At the time the Court Monitor submits his or her periodic reports to the court, the Monitor shall separately list his or her *ex parte* communications with the Parties.

7. **Engagement of Staff and Consultants:** The Court Monitor may, consistent with a budget to be approved by the court, hire staff or expert consultants to assist the Court Monitor in performing his or her duties. The Court Monitor will provide the Parties advance written notice of his or her intention to hire a particular consultant, and such notice will include a resume and a description of duties of the consultant.

8. **Compensation, and Expenses:** Microsoft shall fund the Court Monitor's work pursuant to invoices submitted by the Court Monitor. The Court Monitor shall incur only such fees and expenses as may be reasonably necessary to fulfill the Court Monitor's duties under this Order, or such other orders as the court may issue. Every 120 days, in connection with reports of communications set forth above, the Court Monitor shall submit to the court an itemized statement of fees and expenses paid in connection with the Court Monitor's duties, which the

court will inspect for regularity and reasonableness.

9. Other Provisions: As an agent and officer of the court, the Court Monitor and those working at his or her direction shall enjoy the same protections from being compelled to give testimony and from liability for damages as those enjoyed by other federal judicial adjuncts performing similar functions. Nevertheless, any Party or non-party may request that the court direct the Court Monitor to disclose documents or other information reasonably necessary to an investigation or the litigation of legal claims in another judicial forum that are reasonably related to the Court Monitor's work under this Order. The Court shall not order the Court Monitor to disclose any information without providing the Parties notice and an opportunity to be heard. As required by Rule 53(b)(2) of the Federal Rules of Civil Procedure, the court directs the Court Monitor to proceed with all reasonable diligence. The Court Monitor shall be discharged or replaced only upon an order of the Court. The parties, their successors in office, agents, and employees will observe faithfully the requirements of this Order and cooperate fully with the Court Monitor, and any staff or expert consultant employed by the Court Monitor, in the performance of their duties.

10. Retention of Jurisdiction: The Court will retain jurisdiction to enforce and modify this Order until such time as the Court finds that Microsoft does not seek further determinations regarding any additional Phosphorus Domains or that Defendants establish, by a preponderance of the evidence, that there is no risk of continued use of Phosphorus Domains in violation of the Preliminary Injunction. Under no circumstances will the court's jurisdiction to modify or enforce this Order lapse before January 1, 2030.

IT IS FURTHER ORDERED that copies of this Order and all other pleadings and documents in this action, including orders, determinations, reports and recommendations of the

Court Monitor, may be served by any means authorized by law, including (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to Defendants' domain registrars and/or hosting companies and as agreed to by Defendants in the domain registration or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the U.S.; (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent Defendants provided accurate contact information in foreign countries that are signatory to such treaties.

IT IS SO ORDERED

Entered this __ day of July, 2019

_____

Amy Berman Jackson
United States District Judge