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

MICROSOFT CORPORATION, *Plaintiff,* v. JOHN DOES 1-2, *Defendants.*	Case No. 1:19-cv-01582 Hon. Liam O'Grady

ORDER

This matter comes before the Court on the Report and Recommendation issued by Magistrate Judge John F. Anderson on November 20, 2020. Dkt. 43. Pursuant to Fed. R. Civ. P 72(b), the deadline for submitting any objections to the Report and Recommendation was December 8, 2021. No objections were filed.

Having reviewed the record and the Report and Recommendation, the Court hereby **APPROVES** and **ADOPTS** the Recommendation set forth therein. Accordingly, the Plaintiff's Motion for Default Judgment and Permanent Injunction, Dkt. 38, is hereby **GRANTED**.

It is hereby **ORDERED** that Defendants are in default, and that judgment is awarded in favor of Plaintiff and against Defendants.

It is further **ORDERED** that Defendants, Defendants representatives, and persons who are in active concert or participation with Defendants are permanently restrained and enjoined from (1) intentionally accessing and sending malicious software or code to Microsoft and the protected computers and operating systems of Microsoft and Microsoft's customers, without authorization,

in order to infect those computers; (2) intentionally attacking and compromising computers or computer networks of Microsoft or Microsoft's customers, to monitor the activities of the owners or users of those computers or computer networks, and to steal information from those computers or networks; (3) configuring, deploying, operating, or otherwise participating in or facilitating a command and control infrastructure, or any component or element of the command and control infrastructure at any location; (4) stealing information from Microsoft's customers; (5) misappropriating that which rightfully belongs to Microsoft, its customers, or in which Microsoft or its customers have a proprietary interest; (6) downloading or offering to download additional malicious software onto the computers of Microsoft's customers; or (7) undertaking any similar activity that inflicts harm on Microsoft, Microsoft's customers, or the public including but not limited through the Internet domains set forth in Appendix A or any other "Thallium Domain," as further defined below.

It is further **ORDERED** that Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants are permanently restrained and enjoined from (1) using and infringing Microsoft's trademarks, trade names, service marks, or Internet Domain addresses or names to carry out the enjoined activity; (2) using in connection with Defendants' activities, products, or services any false or deceptive designation, representation or description of Defendants or of their activities, whether by symbols, words, designs or statements, which would damage or injure Microsoft or give Defendants an unfair competitive advantage or result in deception of consumers; or (3) acting in any other manner which suggests in any way that Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Microsoft, or passing off Defendants' activities, products or services as Microsoft's.

It is further **ORDERED** that Defendants shall forfeit ownership and control of all domains

used to carry out the activities enjoined herein, including the domains identified at Appendix A and Appendix B, and any other "Thallium Domain," as further defined below.

It is further **ORDERED** that, pursuant to the All Writs Act (28 U.S.C. § 1651) that the terms of this Permanent Injunction shall be enforced against the Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants, as follows:

1. With respect to the domains set forth at Appendix A and any registered Internet domains that are determined to be "Thallium Domains," through the process set forth in this Order, and where the relevant domain registry is located in the United States, the domain registry shall take the following actions:

   A. Within five (5) business days of receipt of this Order, the domain registries shall unlock and change the registrar of record for the domains 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 domains under its control, the domain registry for the domains, 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 domains 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 domains 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 domains 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 domains.

C. The domains shall be redirected by Microsoft to secure servers by changing the authoritative name servers to NS096A.microsoftinternetsafety.net and NS096B.microsoftinternetsafety.net and, as may be necessary, other name servers or IP addresses associated with name servers and the domain registries shall take reasonable steps to work with Microsoft to ensure the redirection of the domains and to ensure that Defendants cannot use them 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 War
Redmond, WZ 98052
United States
Phone: +1.4258828080
Facsimile: +1.4259367329

E. The domains should be maintained in a manner to 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. All required steps should be taken to propagate the foregoing changes through the Domain Name System ("DNS"), including domain registrars.

2. With respect to any registered Internet domains that are determined to be "Thallium Domains," through the process set forth in this Order, and where the relevant domain registry is located outside of the United States, any such non-U.S. domain registry is respectfully requested, but is not ordered, to provide assistance to Microsoft to prevent the Defendants' use of the domains 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 this Permanent Injunction.

It is further **ORDERED** that "Thallium Domains" are domains which are determined to meet the following two criteria:

1. The domains are used by the Defendants to break into computers and networks of the organizations that Thallium 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 this Permanent Injunction. A domain is determined to be a Thallium Domain by comparing the activities and patterns associated with that domain with known confirmed Thallium Domains. The following factors concerning the domain will be used in this analysis:
   A. Delivers malicious software, code, commands, exploits, implants and/or "backdoor" functionality previously associated with Thallium, including but not limited to: BabyShark, KimJongRAT, PCRat and Gh0st RAT, Cowboy Loader, Cowboy Converter malware, or similar code or functionality deployed in a manner previously associated with Thallium.
   B. 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 Thallium or similar code or functionality.

C. Domain interaction with and similar observation of known Thallium infrastructure.

D. Registration and domain name patterns.

E. Structure of domain name, subdomain and/or file path previously associated with Thallium.

F. Keywords or organization names previously associated with Thallium.

G. Domain registration information previously associated with Thallium.

H. Payment mechanisms and patterns previously associated with Thallium.

I. Name servers.

J. Start of Authority (SOA) records.

K. Resolves to IP of past Thallium domain, malware, command and control server or similar infrastructure.

L. Hosted content previously associated with Thallium.

M. Used to deceive, target, obtain information from, and/or communicate commands or code to recipients, persons, institutions or networks previously targeted by Thallium.

N. 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, think tanks, universities, journalists, political advisors or organizations, government bodies, diplomatic institutions, and/or military forces and installations.

O. SSL Cert Issuer_DN.

P. SSL Cert Subject_DN.

Q. Host.

R. Registrar.

2. The Defendants' activities associated with the domains, malicious code or software associated with the domains, domain names or content associated with 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: "Access," "Active Directory," "ActiveX" "AppLocker," "Authenticode," "Azure," "Bing," "BitLocker," "BizSpark," "BizTalk," "BlueTrack," "BranchCache," "CodeLens," "Cortana," "Delve," "DeployR," "DevelopR," "Direct3D," "DirectX," "DistributedR," "DreamSpark," "Dynamics," "Edge," "Excel," "Exchange," "ExpressRoute," ForeFront," "GroupMe," "HDInsight," "Healthvault," "HoloLens," "Hotmail,"

"Hyper-V," "InfoPath," "InPrivate," "IntelliMirror," "IntelliSense," "IntelliTrace," "InterFlow," "Internet Explorer," "JScript," "Kinect," "LifeCam," "LifeChat," "LightSwitch," "Live," "Lumia," "Lync," "Microsoft," "Minecraft," "MSDN," "MSFT," "MS," "MSN," "MultiPoint," "O365," "Office," "Office 365," "OneDrive," "OneNote," "Outlook," "OWA," "Passport," "PlayReady," "PowerApps," "Power BI," "PowerPoint," "PowerShell," "Publisher," "RemoteFX," "ScaleR," "SharePoint," "Silverlight," "Skype," "SmartGlass," "SmartScreen," "SQL Server," "StorScore," "StorSimple," "Surface," "Sway," "SwiftKey," "SyncToy," "U-SQL," "Visio," "Visual Basic," "Visual C++," "Visual C#," "Visual F#," "Visual J++," "Visual J#," "Visual Studio," "Win," "WebMatrix," "Windows," "Word," "Xamarin," "Xbox and Yammer," and any confusingly similar variants of any of the foregoing. 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, with respect to domains alleged to meet the criteria to constitute Thallium Domains and domains that are alleged to be Thallium Domains based on new criteria not listed in this Order, Microsoft shall submit a written motion to this Court or the Court Monitor seeking a declaration that such domains are Thallium Domains. This Court or the Court Monitor shall take and hear evidence and shall make determinations and issue orders whether domains are Thallium Domains, as set forth further below.

It is further **ORDERED** that, pursuant to Federal Rule of Civil Procedure 53(a)(1)(C) and the court's inherent equitable powers, Hon. S. James Otero (Ret.) is appointed to serve as Court Monitor in order to make determinations on disputes regarding whether particular domains are Thallium Domains, to make determinations and orders regarding whether particular domains are

Thallium Domains, and to monitor Defendants' compliance with the Permanent Injunction. The Court Monitor has filed 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), and the record shows no grounds for disqualification. The following sets forth the terms of the appointment of the Court Monitor:

1. The duties of the Court Monitor shall include:
    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 Thallium Domains and, with respect to motions submitted by Microsoft that particular domains constitute Thallium Domains, making determinations whether such domains are or are not Thallium 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 Permanent Injunction;
2. The Court Monitor shall have all authority provided under Federal Rule of Civil

Procedure 53(c).

3. The Court Monitor shall resolve objections and shall make determinations and issue orders whether domains are Thallium Domains, pursuant to the terms set forth in the Permanent Injunction 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 Thallium Domains, or upon receipt of a written motion from Microsoft for a finding that particular domains constitute Thallium Domains, the Court Monitor shall take and hear evidence whether a domain is a Thallium 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 Thallium Domains. Accordingly, in furtherance of this purpose, all objections, motions and responses shall be embodied and communicated betw 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. 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. § 1651(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 periodic reports to the court, as set forth below, the Monitor shall separately list in summary form uncontested orders and determinations.

4. 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.

5. 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.

6. The Court Monitor shall provide periodic reports to the court and to the Parties concerning the status of Defendants' compliance with the Permanent Injunction 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.

7. 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.

8. The Court Monitor may 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.

9. Microsoft shall fund the Court Monitor's work. 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 60 days the Court Monitor shall submit to Microsoft an itemized statement of fees and expenses. Microsoft shall pay such fees and expenses within 30 calendar days of receipt. The Court Monitor shall file such statements of fees and expenses with the reports set forth in Paragraph 5 above. If Microsoft disputes a statement, the Court monitor shall submit the statement the court. The court will inspect any such disputed statement for regularity and reasonableness, make determinations regarding what portion of the statement is regular and reasonable, sign and transmit such finalized statement to Microsoft. Microsoft shall then remit to the Court Monitor any court-approved amount of any disputed statement, within 30 calendar days of court approval.

10. As an agent and officer of the court, the Court Monitor and those working at the Court Monitor's 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.

11. The Court will retain jurisdiction to enforce and modify the Permanent Injunction and this Order until such time as the Court finds that Microsoft does not seek further determinations regarding any additional Thallium Domains or that Defendants establish, by a preponderance of the evidence, that there is no risk of continued use of Thallium Domains in violation of the Permanent Injunction.

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 further **ORDERED** that the bond posted by Microsoft related to this matter be released.

It is **SO ORDERED.**

April 5, 2021
Alexandria, Virginia

Liam O'Grady
United States District Judge