UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----------X

MICROSOFT CORPORATION, a Washington Corporation, FORTRA, LLC, a Minnesota Corporation, and HEALTH-ISAC, INC., a Florida Corporation,

Plaintiffs,

-against-

JOHN DOES 1-2, JOHN DOES 3-4 (AKA CONTI RANSOMWARE GROUP), JOHN DOES 5-6 (AKA LOCKBIT RANSOMWARE GROUP), JOHN DOES 7-8 (AKA DEV-0193), JOHN DOES 9-10 (AKA DEV-0206), JOHN DOES 11-12 (AKA DEV-0237), JOHN DOES 13-14 (AKA DEV-0243), JOHN DOES 15-16 (AKA DEV-0504), Controlling Computer Networks and Thereby Injuring Plaintiffs and Their Customers,

Defendants.

----------X

ORDER ADOPTING REPORT & RECOMMENDATION

23-CV-2447 (RER) (LKE)

RAMÓN E. REYES, JR., United States District Judge:

In a report and recommendation dated August 6, 2025, (ECF No. 55 (the "R&R")), Magistrate Judge Lara E. Eshkenazi recommended that the Court grant Plaintiffs' motion for default judgment and convert the terms of the preliminary injunction and supplemental preliminary injunctions into a permanent injunction, as outlined in Microsoft's proposed order. (*Id.* at 25; ECF No. 50-2). Judge Eshkenazi advised the parties that they had fourteen days from the date that R&R was received to file objections. (R&R at 25). To date, neither party has filed an objection to the R&R, and the time to do so has passed. *See* Fed. R. Civ. P. 72(b)(2).

Pursuant to 28 U.S.C. § 636(b) and Federal Rule of Civil Procedure 72, the Court has reviewed the R&R for clear error and, finding none, adopts the R&R in its entirety.

See Covey v. Simonton, 481 F. Supp. 2d 224, 226 (E.D.N.Y. 2007). Therefore, it is ordered that the R&R is adopted in its entirety.

IT IS THEREFORE ORDERED that, Microsoft's Motion for Default Judgment and Entry of a Permanent Injunction is Granted.

IT IS FURTHER ORDERED that Defendants are in default, and that judgment is awarded in favor of Microsoft 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 the following actions:

A. Using unauthorized versions of Cobalt Strike to brutally force access into victims' computers; using unauthorized versions of Cobalt Strike to operate a global malware and ransomware infrastructure, using unauthorized versions of Cobalt Strike to deploy malware and ransomware to victims' machines; using unauthorized version of Cobalt Strike to offer RaaS to other malicious actors; using the Conti and LockBit ransomware deployed via unauthorized Cobalt Strike to run and add its own protocols to the Microsoft operating system to go through the list of services and terminates services that are related to backup and recoveries as well as terminating security processes related to operating tool, which causes hundreds of lines of Microsoft's declaring code and the structure, sequence, and organization of that code are copied with and across unauthorized, cracked Cobalt Strike modules and ransomware like LockBit; using the infected victims' computers to send commands and instructions to the infected computing device to control it surreptitiously and deliver malware that, among other things, enables Defendants to take control of the victim's computer and extort money from them.

Defendants' primary goal is to deliver ransomware and enable attacks against other computers; or stealing information, money or property from Plaintiffs, Plaintiffs' customers or Plaintiffs' member organizations, or undertaking any similar activity that inflicts harm on Plaintiffs, or the public, including Plaintiffs' customers or associated member organizations

B. Configuring, deploying, operating or otherwise using or unauthorized Cobalt Strike to facilitate the deployment of defendants' malware and ransomware activities described in the TRO Application, including but not limited to the C2 infrastructure hosted at and operating through the domains and IP addresses set forth herein and through any other deployments of unauthorized Cobalt Strike in any location.

C. Using the trademarks or logos "Microsoft" or "Windows" the logos and trademarks "Cobalt Strike," the trademarks, brands or logos of healthcare institution members of Health-ISAC; and/or other trademarks; trade names; service marks; or Internet domain addresses or names; or acting in any other manner which suggests in any way that Defendants' products or services come from or are somehow sponsored or affiliated with Plaintiffs or Plaintiffs' associated member organizations, and from otherwise unfairly competing with Plaintiffs, misappropriating that which rightfully belongs to Plaintiffs or Plaintiffs' customers or Plaintiffs' associated member organizations, or passing off their goods or services as Plaintiffs or Plaintiffs' associated member organizations.

D. Infringing Plaintiffs' registered trademarks, as set forth in Appendix B and E to the Complaint.

E. Using in connection with Defendants' activities any false or deceptive designation, representation or description of Defendants' or of their representatives' activities, whether by symbols, words, designs or statements, which would damage or injure Plaintiffs or give Defendants an unfair competitive advantage or result in deception of consumers.

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

A. With respect to the domains set forth at Appendix A and any registered Internet domains that are determined to be "Cobalt Strike 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:

1. Within three (3) 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.

2. 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;

3. The domain registries shall take reasonable steps to work with Microsoft to ensure the transfer 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 this Order;

4. 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

Email: domains@microsoft.com

5. 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;

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

B. With respect to any of the IP Addresses set forth in Appendix A to this Order, the data centers and/or hosting providers identified in Appendix A to this Order, A and any registered IP addresses that are determined to be "Cobalt Strike IP Addresses," and associated data centers and/or hosting providers shall take reasonable best efforts to implement the following actions:

1. Take reasonable steps to identify incoming and/or outgoing Internet traffic on their respective networks associated with Defendants that originates and/or is being sent from and/or to the IP Addresses identified in Appendix A;

2. Take reasonable steps to block incoming and/or outgoing Internet traffic on their respective networks associated with Defendants that originate and/or are being sent from and/or to the IP Addresses identified in Appendix A, by Defendants or Defendants' representatives or resellers, except as explicitly provided for in this Order;

3. Completely disable the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with Defendants' use of the IP Addresses set forth in Appendix A and make them inaccessible from any other computer on the Internet, any internal network,

or in any other manner, to Defendants, Defendants' representatives and all other persons, except as otherwise ordered herein;

4. Completely, and until further order of this Court, suspend all services to Defendants or Defendants' representatives or resellers associated with the IP Addresses set forth in Appendix A;

5. Isolate and disable any content and software associated with the Defendants hosted at the IP Addresses listed in Appendix A in a manner that does not impact any content or software not associated with Defendants hosted at the IP Addresses listed in Appendix A. In determining the method and mechanism to disable content and software associated with the Defendants, the relevant data centers and/or hosting providers shall reasonably confer with Plaintiffs' counsel, Jeffrey L. Poston, Crowell & Moring LLP, 1001 Pennsylvania Ave. NW, Washington D.C., 20004, jposton@crowell.com, to facilitate any follow-on action;

6. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from publicizing this Order until this Order is executed in full, except as necessary to communicate with hosting companies, data centers, the Plaintiffs or other ISPs to execute this order; 7. Not enable, and shall take all reasonable steps to prevent, any circumvention of this order by Defendants or Defendants' representatives associated with the IP Addresses, including without limited to enabling, facilitating, and/or allowing Defendants or Defendants' representatives or resellers to rent, lease, purchase, or otherwise obtain

another IP Address associated with your services; 8. Preserve, retain and produce to Plaintiffs all documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling the IP Addresses set forth in Appendix A, including any and all individual or entity names, mailing addresses, e-mail addresses, facsimile numbers and telephone numbers or similar contact information, including but not limited to such contact information reflected in billing, usage, access and contact records and all records, documents and logs associated with Defendants' or Defendants' Representatives' use of or access to the IP Addresses; 9. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order; and 10. Completely preserve the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with the IP Addresses set forth in Appendix A, and preserve all evidence of any kind related to the content, data, software or accounts associated with such IP addresses and such computer hardware, such that such evidence of Defendants' unlawful activities is preserved.

IT IS FURTHER ORDERED that "Cracked Cobalt Strike Domains" are domains which are determined to meet the following criteria:

Criteria 1: The domains are used by Defendants to break into computers and networks of the organizations that Cracked Cobalt Strike targets, or control the reconnaissance of those networks, or, ultimately, exfiltrate sensitive information from them, or are otherwise used by Defendants to carry out the activities and

purposes prohibited by this Permanent Injunction. A domain is determined to be a Cracked Cobalt Domain/ by comparing the activities and patterns associated with known behaviors of the Cracked Cobalt Strike. The following factors will be used:

Use of Ransomware that is associated with Cracked Cobalt Strike	Uses Cracked Cobalt Strike as go-to tools for Ransomware as a Service (RaaS), often leveraging Conti, Lockbit, Quantum Locker, Royal, Cuba, BlackBasta BlackCat, and PlayCrypt families.
Association with DEV-0193 threat group	Develops, distributes, and manages many different payloads, including Trickbot, Bazaloader, and AnchorDNS. Also manages ransomware as a service (RaaS) programs that are developed as a result of leveraging cracked Cobalt Strike Beacons to drop ransomware payloads.
Association with DEV-0206 threat group	Access broker that uses malvertising technique to gain access to and profile networks using Cobalt Strike payloads and in numerous instances, led to custom cracked Cobalt Strike loaders created by malware families.

Association with DEV-0237 threat group	Prolific ransomware as a service affiliate that alternates between different payloads in their operations based on what is available. Uses the cybercriminal gig economy to also gain initial access to networks. Leverages cracked Cobalt Strike Beacons dropped by the malware they purchased to conduct reconnaissance.
Association with DEV-0243 threat group	EvilCorp group that develops Cobalt Strike loaders for other malware campaigns.
Association with DEV-0504 threat group	Relies on access brokers to enter a network, using Cobalt Strike beacons they purchased access to, to move laterally and stage their payloads. They frequently disable antivirus products that are not protected with tamper protection
Engages in the following built-in commands that are implemented via modules (DLL)	Screenshots, desktop control, keylogger, mimikatz, credential and hash harvesting, malleable command and control design and reference guide.

Copies portions of Microsoft code	Cobalt Strike's malicious software's "beacon.dll" file copies literal code and the structure sequence and organization of Windows code such as the GetUserObjectInformationA, RegCloseKey, LookupAccountSid, CryptGenRandom, LogonUserA, AdjustTokenPrivileges, ReadProcessMemory, TerminateProcess, CopyFileA, HttpSendRequestA code, and many other Windows code elements. Additionally, reproduces the copyrighted Microsoft declaring code, that is part of the Microsoft application programming interfaces ("APIs")
Domains similar to previously used domains or IP addresses	Victims being targeted similar to past targets

Criteria 2: The domains (a) use and infringe Microsoft's, Health-ISAC's, or Fortra'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 Plaintiffs 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 Plaintiffs, or pass off Defendants' activities, products or services as Plaintiffs'. Criteria 2 is also met where Defendants use generalized versions of terms that are suggestive of Plaintiffs' products and services, but do not specifically use a trademark.

IT IS FURTHER ORDERED that "Cracked Cobalt IP addresses" are IP addresses which are determined to meet the following criteria: Criteria 1: The IP addresses are used by Defendants to break into computers and networks of the organizations that Cracked Cobalt Strike targets, or control the reconnaissance of those networks, or, ultimately, exfiltrate sensitive information from them, or are otherwise used by Defendants to carry out the activities and purposes prohibited by this Permanent Injunction. An IP address is determined to be a Cracked Cobalt IP address by comparing the activities and patterns associated with known behaviors of the Cracked Cobalt Strike. The following factors will be used:

Use of Ransomware that is associated with Cracked Cobalt Strike	Uses Cracked Cobalt Strike as go-to tools for Ransomware as a Service (RaaS), often leveraging Conti, Lockbit, Quantum Locker, Royal, Cuba, BlackBasta BlackCat, and PlayCrypt families.
Association with DEV-0193 threat group	Develops, distributes, and manages many different payloads, including Trickbot, Bazaloader, and AnchorDNS. Also

	manages ransomware as a service (RaaS) programs that are developed as a result of leveraging cracked Cobalt Strike Beacons to drop ransomware payloads.
Association with DEV-0206 threat group	Access broker that uses malvertising technique to gain access to and profile networks using Cobalt Strike payloads and in numerous instances, led to custom cracked Cobalt Strike loaders created by malware families.
Association with DEV-0237 threat group	Prolific ransomware as a service affiliate that alternates between different payloads in their operations based on what is available. Uses the cybercriminal gig economy to also gain initial access to networks. Leverages cracked Cobalt Strike Beacons dropped by the malware they purchased to conduct reconnaissance.
Association with DEV-0243 threat group	EvilCorp group that develops Cobalt Strike loaders for other malware campaigns.
Association with DEV-0504 threat group	Relies on access brokers to enter a network, using Cobalt Strike beacons they

	purchased access to, to move laterally and stage their payloads. They frequently disable antivirus products that are not protected with tamper protection
Engages in the following built-in commands that are implemented via modules (DLL)	Screenshots, desktop control, keylogger, mimikatz, credential and hash harvesting, malleable command and control design and reference guide.
Copies portions of Microsoft code	Cobalt Strike's malicious software's "beacon.dll" file copies literal code and the structure sequence and organization of Windows code such as the GetUserObjectInformationA, RegCloseKey, LookupAccountSid, CryptGenRandom, LogonUserA, AdjustTokenPrivileges, ReadProcessMemory, TerminateProcess, CopyFileA, HttpSendRequestA code, and many other Windows code elements. Additionally, reproduces the copyrighted Microsoft declaring code, that is part of the Microsoft application programming interfaces ("APIs")

Domains similar to previously used domains or IP addresses	Victims being targeted similar to past targets

IT IS FURTHER ORDERED that pursuant to Federal Rule of Civil Procedure 53(a)(1)(C) and the court's inherent equitable powers, Hon. James Otero (Ret.) is appointed to serve as Court Monitor in order to make determinations on disputes regarding whether particular domains or IP addresses are Cobalt Strike Domains or IP addresses, to make determinations and orders regarding whether particular domains/IP addresses are Cobalt Strike Domains or IP addresses, and to monitor Defendants' compliance with the Permanent Injunction. The following set forth the terms of the appointment of the Court Monitor:

A. Duties: the duties of the Court Monitor shall include the following:

1. Carrying out all responsibilities and tasks specifically assigned to the Court Monitor in this Order;

2. Resolving objections submitted by domain registries or IP hosting providers, Defendants or other third parties, to Plaintiffs' determinations that domains/IP addresses constitute Cobalt Strike Domains or IP addresses and, with respect to motions submitted by Plaintiffs that particular domains/IP addresses constitute Cobalt Strike Domains or IP addresses, making determinations whether such domains/IP addresses are or are not Cobalt Strike Domains or IP addresses.

3. 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;

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

5. Monitoring and reporting on Defendants' compliance with their obligations under the Permanent Injunction;

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

B. Orders Regarding Cobalt Strike Domains or IP Addresses: The Court Monitor shall resolve objections and shall make determinations and issue orders whether domains/IP addresses are Cobalt Strike Domains or IP addresses pursuant to the terms set forth in the Permanent Injunction and pursuant to the following process:

1. Upon receipt of written objects from any domain registries or IP hosting providers Defendants or any other third parties contesting any determinations by Plaintiffs that particular domains/IP addresses constitute Cobalt Strike Domains or IP addresses, or upon receipt of a written motion from Plaintiffs for a finding that particular domains/IP address constitute Cobalt Strike Domains or IP address, the Court Monitor shall take and hear evidence whether a domain/IP address is a Cobalt Strike Domain or IP address, 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 this Court or 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. This Court or 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 this Court or the Court Monitor may order provisional relief, including redirection of domains, blocking of specific IP address ports, or other temporary disposition of domains/IP addresses, while any objection or motion is pending.

2. It is the express purpose of this order to afford prompt and efficient relief and disposition of Cobalt Strike Domains or IP addresses. 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 this Court or the Court Monitor. Also in furtherance of this purpose, hearings shall be telephonic or in another expedited form as may be reasonably specified by this Court or the Court Monitor.

3. This Court or 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 and/or IP hosting providers).

4. This Court and the Court Monitor are 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. 5. 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 this Court, as set forth below, the Monitor shall separately list in summary form uncontested orders and determinations.

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

1. 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.

2. 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).

3. Any party may seek and the Court may order provisional relief, redirection of domains, blocking of specific IP address ports, or other temporary disposition of domains/IP addresses, while any objection or motion is pending.

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

5. 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.

D. 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.

E. Periodic Reporting: 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.

F. 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.

G. Engagement of Staff and Consultants: 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.

H. 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.

I. Other Provisions: 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.

J. Retention of Jurisdiction: 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 Cobalt Strike Domains or IP addresses or Defendants establish, by a preponderance of the evidence, that there is no risk of continued use of Cobalt Strike Domains or IP addresses in violation of the Permanent 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 may be served by any means authorized by law, including any one or combination of (1) personal delivery upon Defendants who provided accurate contact information in the U.S., if any; (2) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided accurate contact information in foreign countries that are signatory to such treaties, if any, (3) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their hosting companies and as agreed to by Defendants in their hosting agreements, (4) publishing notice on a publicly available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

The Clerk of Court is directed to enter default judgment against defendants.

SO ORDERED.

/s/ Ramón E. Reyes, Jr. 10:06 A.M.

RAMÓN E. REYES, JR.
United States District Judge

Dated: September 8, 2025
Brooklyn, NY