UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

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

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.

Case No. 23-cv-2447-LDH-JRC

FILED UNDER SEAL

***EX PARTE* TEMPORARY RESTRAINING ORDER, SEIZURE ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

Plaintiffs Microsoft Corp. ("Microsoft"), Fortra LLC ("Fortra"), and Health-ISAC, Inc. ("Health-ISAC") have filed a Complaint for injunctive and other relief pursuant to, Digital Millennium Copyright Act (17 U.S. § 1201); the Copyright Act (17 U.S.C. §§ 101 *et seq.*); the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); violations of the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); conspiracy to violate the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); and the common law of trespass, conversion, and unjust enrichment. Plaintiffs have also moved *ex parte* for an emergency temporary restraining order and seizure order pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C § 1116(d) (the "Lanham Act") and 28 U.S.C. § 1651(a) (the "All Writs Act"), and an order to show cause why a preliminary injunction should not be granted.

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Plaintiffs' Application for an Emergency Temporary Restraining Order, Seizure Order, and Order to Show Cause for Preliminary Injunction ("TRO Application"), the Court hereby makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against Defendants under the Digital Millennium Copyright Act (17 U.S. § 1201); the Copyright Act (17 U.S.C. §§ 101 *et seq.*); the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); violations of the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); conspiracy to violate the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); and the common law of trespass, conversion, and unjust enrichment.

2. Microsoft owns the registered trademarks "Microsoft" and "Windows" used in connection with its services, software, and products. Copies of the trademark registrations

for the Microsoft marks are attached as **Appendix B** to the Complaint.

3. Microsoft also owns copyrights in the code, documentation, specifications, libraries, and other materials that comprise the Windows operating system, including the Declaring Code (the code at issue in this case encompasses a type of code called "declarations" within header files and within libraries contained in the software development kit ("SDK")). Specifically, Microsoft owns the registered copyrights in the Windows 8 SDK, Reg. No. TX 8-999-365 (Copyrighted Work). Microsoft's Copyrighted Work is an original, creative work and copyrightable subject matter under the laws of the United States. Copies of the registration are attached to the Complaint as **Appendix C**.

4. Fortra also owns the copyrights in the code, documentation, specifications, libraries, and other materials that comprise the Cobalt Strike proprietary software. Fortra's copyrights are registered with the United States Copyright Office. Copies of the registration are attached to the Complaint as **Appendix D**.

5. Fortra owns the registered trademark in Cobalt Strike. Copies of the trademark registration for Fortra are attached to the Complaint as **Appendix E.**

6. Health-ISAC's members have invested in developing their brands, trademarks and trade names in association with the healthcare industry. Health-ISAC represents the interests of its members in maintaining security and maintaining their brand integrity regarding security matters.

7. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate Digital Millennium Copyright Act (17 U.S. § 1201); the Copyright Act (17 U.S.C. §§ 101 *et seq.*); the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); violations of the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); conspiracy to violate the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); and the common law of trespass, conversion, and unjust enrichment.

8. There is good cause to believe that, unless Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from Defendants' ongoing violations of the Digital Millennium Copyright Act (17 U.S. § 1201); the Copyright Act (17 U.S.C. §§ 101 *et seq.*); the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); violations of the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); conspiracy to violate the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); and the common law of trespass, conversion, and unjust enrichment. The evidence set forth in Plaintiffs' TRO Application and the accompanying declarations and exhibits, demonstrates that Plaintiffs are likely to prevail on their claim that Defendants have engaged in violations of the foregoing laws by: (1) using cracked versions of the Cobalt Strike software[1] to force their way into victim machines; (2) once inside the victims' machines, use unauthorized versions of Cobalt Strike to deploy ransomware and malware; (3) crippling victims' machines computer infrastructure and/or deleting files to force the payment of ransom from the victims; (4) stealing personal account information from users; (5) using the stolen personal information to carryout further illegal acts; (6) operate as a Ransom as a Service ("RaaS") model whereby affiliates pay to Defendants to launch ransomware attacks developed by other operators; and (7) associating with one another in a common enterprise engaged in these illegal acts. There is good cause to believe that if such conduct continues, irreparable harm will occur to Plaintiffs and the public, including Plaintiffs' customers and associated member organizations. There is good cause to believe that the Defendants are engaging, and will continue to engage, in such unlawful actions if not immediately restrained from doing so by Order of this Court.

9. There is good cause to believe that the malicious use of unauthorized Cobalt Strike software infringes Microsoft's copyright by copying literal lines of Microsoft Windows code, commands, system files, and file structures, and the structure, sequence, and organization of such code. For example, the malicious software's "beacon.dll" file copies literal code and the structure sequence and organization

[1] As used in this action, "cracked versions of Cobalt Strike" refer to stolen, unlicensed, or otherwise unauthorized versions or copies of Cobalt Strike.

of Windows code such as the GetUserObjectInformationA, RegCloseKey, LookupAccountSid, CryptGenRandom, LogonUserA, AdjustTokenPrivileges, ReadProcessMemory, TerminateProcess, CopyFileA, HttpSendRequestA code, and many other Windows code elements.

10. There is good cause to believe that the malicious use of unauthorized Cobalt Strike also infringes Fortra's copyright by literally copying the entirety of its copyrighted Cobalt Strike "team server" code in a cracked, unauthorized version used for malicious purposes. The infringement involves unauthorized copying of executable code for all of the Cobalt Strike team server's web server, beacon and configuration features and functionality, including all of Fortra's creative and original method implementations, interfaces, parameters, variables, arrays, data types, operators, and objects.

11. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of the unauthorized Cobalt Strike command and control ("C2") infrastructure that is hosted at and otherwise operates through the Internet domains listed in **Appendix A** or through the Internet Protocol ("IP") addressees, also listed in **Appendix A**, and from the destruction or concealment of other discoverable evidence of Defendants' misconduct available at those locations if Defendants receive advance notice of this action. Based on the evidence cited in Plaintiffs' TRO Application and accompanying declarations and exhibits, Plaintiffs are likely to be able to prove that: (1) Defendants are engaged in activities that directly violate U.S. law and harm Plaintiffs and the public, including Plaintiffs' customers and member-organizations; (2) Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests; (3) Defendants are likely to delete or relocate the command and control software at issue in Plaintiffs' TRO Application and the harmful, malicious, and trademark infringing software disseminated through these IP addresses and domains and to warn their associates engaged in such activities if informed of Plaintiffs' action. Plaintiffs' request for this emergency *ex parte* relief is not the result of any lack of diligence on Plaintiffs' part, but instead is based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b) and 15 U.S.C. § 1116(d), good cause and the interests of justice require that this Order be granted without prior notice to Defendants, and accordingly Plaintiffs are relieved of the duty to provide Defendants with prior notice of Plaintiffs' motion.

12. There is good cause to believe that Defendants have specifically directed their activities to computers of Plaintiffs' customers and member organization located in the Eastern District of New York.

13. There is good cause to believe that Defendants have engaged in illegal activity using the data centers and/or Internet hosting providers identified in Appendix A to host the unauthorized Cobalt Strike C2 infrastructure used to maintain and operate the unauthorized Cobalt Strike software at computers, servers, electronic data storage devices or media at the IP addresses identified in Appendix A.

14. There is good cause to believe that to immediately halt the injury caused by Defendants, data and evidence at Defendants' IP addresses identified in Appendix A must be preserved and held in escrow pending further order of the court, Defendants' computing resources related to such IP addresses must then be disconnected from Defendants' infrastructure, Defendants must be prohibited from accessing Defendants' computer resources related to such IP addresses and the data and evidence located on those computer resources must be secured and preserved.

15. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains identified in Appendix A to this order to host the command and control software and content used to maintain and operate the Defendants' harmful infrastructure. There is good cause to believe that to immediately halt the injury caused by Defendants, each of Defendants' current and prospective domains set forth in Appendix A must be immediately transferred to the control of Microsoft where they can be secured and thus made inaccessible to Defendants.

16. There is good cause to direct that third party Internet registries, registrars, data centers, and hosting providers with a presence in the United States to reasonably assist in the implementation of this Order and refrain from frustrating the implementation and purposes of this Order, pursuant to 28 U.S.C. § 1651(a) (the All Writs Act).

17. There is good cause to believe that if Defendants are provided advance notice of Plaintiffs' TRO Application or this Order, they would move the Defendants'

infrastructure, allowing them to continue their misconduct and that they would destroy, move, hide, conceal, or otherwise make inaccessible to the Court evidence of their misconduct, the Defendants' infrastructure's activity, the infringing materials, the instrumentalities used to make the infringing materials, and the records evidencing the manufacture and distributing of the infringing materials.

18. There is good cause to permit notice of the instant Order, notice of the Preliminary Injunction hearing and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, satisfy Fed. R. Civ. Pro. 4(f)(3), and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) personal delivery upon Defendants who provided to the data centers and Internet hosting providers contact information in the U.S.; (2) personal delivery through the Hague Convention on Service Abroad or other treaties upon Defendants who provided contact information outside the United States; (3) transmission by e-mail, electronic messaging addresses, facsimile, and mail to the known email and messaging addresses of Defendants and to their contact information provided by Defendants to the domain registrars, registries, data centers, Internet hosting providers, and website providers who host the software code associated with the IP addresses or through which domains are registered, both of which are identified in Appendix A.; and (4) publishing notice to the Defendants on a publicly available Internet website and in newspapers in jurisdictions where Defendants are believed to reside.

19. There is good cause to believe that the harm to Plaintiffs of denying the relief requested in their TRO Application outweighs any harm to any legitimate interests of Defendants and that there is no undue burden to any third party.

TEMPORARY RESTRAINING ORDER AND SEIZURE ORDER

IT IS THEREFORE ORDERED as follows:

A. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from: 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. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from 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. Defendants, their representatives and persons who are in active concert or

participation with them are temporarily restrained and enjoined from 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. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from infringing Plaintiffs' registered trademarks, as set forth in Appendix B and E.

Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from 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, 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 shall take reasonable best efforts to implement the following actions:

A. 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;

B. 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;

C. 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;

D. 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;

E. 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, Gabriel M. Ramsey, Crowell & Moring LLP, 3 Embarcadero Ctr., 26th Floor, San Francisco, CA 94111, gramsey@crowell.com, (Tel: 415-365-7207), to facilitate any follow-on action;

F. 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;

G. 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;

H. 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;

I. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order; and

J. 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, pursuant to the All Writs Act, with respect to any currently registered Internet domain set forth in **Appendix A**, the domain registries shall take the following actions:

A. 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.

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 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;

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 copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint 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.

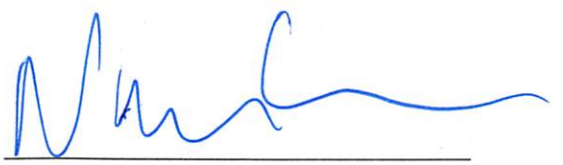
IT IS FURTHER ORDERED, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before the Hon. LaShann DeArcy Hall on April 13, 2023, at 1:00 p.m. to show cause, if there is any, why the Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against the Defendants, enjoining them from the conduct temporarily restrained by the preceding provisions of this Order.

IT IS FURTHER ORDERED that Microsoft, on behalf of Plaintiffs, shall post bond in the amount of $15,000 as cash to be paid into the Court registry.

IT IS FURTHER ORDERED that the Defendants shall file with the Court and serve on Plaintiffs' counsel any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later than two (2) days prior to the hearing on Plaintiffs' request for a preliminary injunction. Plaintiffs may file responsive or supplemental pleadings, materials, affidavits, or memoranda with the Court and serve the same on counsel for the Defendants no later than one (1) day prior to the preliminary injunction hearing in this matter. Provided that service shall be performed by personal or overnight delivery, facsimile or electronic mail, and documents shall be delivered so that they shall be received by the other parties no later than 4:00 p.m. (Eastern Standard Time) on the appropriate dates listed in this paragraph.

IT IS SO ORDERED

Entered this 31st day of March, 2023.



Hon. Nina R. Morrison, U.S.D.J.

(Miscellaneous Duty Judge)