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-02447-LDH-JRC

PRELIMINARY INJUNCTION ORDER

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 moved *for a preliminary injunction* order pursuant to Rule 65(a) 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. On March 31, 2023, the Court issued a temporary restraining order and order to show cause why an injunction should not issue. Defendants have not responded to the Court's Order to show cause.

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. Defendants have not responded to the Court's March 31, 2023 Order to Show Cause.

3. 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, and therefore Plaintiffs are likely to prevail on the merits of this action.

4. Microsoft owns the registered trademarks "Microsoft" and "Windows" used in connection with its services, software, and products.

5. 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.

6. 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.

7. Fortra owns the registered trademark in Cobalt Strike.

8. 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.

9. 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.

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

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

11. 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.

12. There was 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 received advance notice of this action prior to execution of the TRO. 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 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(a),15 U.S.C. § 1116(d), and notice having been given, good cause and the interests of justice require that this Order be granted.

13. There is good cause to believe that the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court.

14. 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.

15. 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.

16. 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.

17. 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.

18. There is good cause to direct 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).

19. There is good cause to permit notice of the instant Order 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.

PRELIMINARY INJUNCTION 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.

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 to the Complaint.

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, that, with respect to any currently registered Internet domains set forth in Appendix A to the Complaint and this Order shall be maintained by Microsoft in its account at the domain registrar MarkMonitor.

IT IS FURTHER ORDERED, that with respect to any currently registered IP addresses set forth in Appendix A to the Complaint and this Order the data centers and/or hosting providers identified in **Appendix A** to the Complaint and this Order shall take reasonable best efforts to ensure that any steps taken by such data centers and/or hosting providers in response to the Temporary Restraining Order shall remain in place during the pendency of this action.

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.

IT IS SO ORDERED

Entered this 19 day of April, 2023.

s/ LDH

The Honorable LaShann DeArcy Hall