

**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

ORDER GRANTING PLAINTIFFS' *EX PARTE* MOTION FOR A SECOND SUPPLEMENTAL PRELIMINARY INJUNCTION ORDER

The Court, having considered the pleadings and declaration in support of Plaintiffs Microsoft Corp. (“Microsoft”), Fortra LLC (“Fortra”), and Health-ISAC, Inc.’s (“Health-ISAC”) (collectively, “Plaintiffs”) Motion for a Second Supplemental Preliminary Injunction Order, hereby orders that the terms of the Preliminary Injunction Order (“Preliminary Injunction Order”), Dkt. No. 20, shall apply to the additional domains set forth in Appendix A to this order. As set forth below, Defendants have continued to violate the Preliminary Injunction.

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Plaintiffs’ Motion to Supplement the Preliminary Injunction Order, the Court hereby makes the following findings of fact and conclusions of law:

1. The Defendants were served with notice of the TRO and Preliminary Injunction via the alternative service methods previously authorized by this Court.

2. After receiving notice of the TRO, Preliminary Injunction Order, and the First Supplemental Preliminary Injunction Order, the Defendants have continued to engage in the conduct that this Court’s Preliminary Injunction Order has enjoined, and therefore continue to violate the Preliminary Injunction Order. In particular, using new domains, Defendants have intentionally and without authorization, continued and attempted to access and send malicious software, code, and instructions to protected computers, operating systems, and networks of Plaintiffs and their customers, attacking such computers, systems and networks, and exfiltrating information from those computers, systems and networks.

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

4. There is good cause to believe that, unless further relief is ordered to expeditiously prevent Defendants from maintaining the domains for purposes enjoined by the Preliminary Injunction Order, immediate and irreparable harm will result to Plaintiffs, their customers, and to

the public, from the Defendants' ongoing violations.

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

SECOND SUPPLEMENTAL PRELIMINARY INJUNCTION

IT IS THEREFORE ORDERED that, the terms of the Preliminary Injunction Order shall be supplemented and shall be enforced against Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants and 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 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 11 day of October 2023.

s/ **LDH**

HON. LASHANN DEARCY HALL
UNITED STATES DISTRICT COURT JUDGE