

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

MICROSOFT CORPORATION,

Plaintiff,

v.

DOES 1-6,

Defendants.

Case No. 1:25-cv-06493-MHC

FILED UNDER SEAL

**TEMPORARY RESTRAINING ORDER
AND ORDER TO SHOW CAUSE**

Before the Court is Plaintiff Microsoft Corporation's motion for a Temporary Restraining Order and Order to Show Cause. Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Plaintiffs' Motion, the Court hereby makes the following findings of fact and conclusions of law:

This Court has jurisdiction over the subject matter of this case and there is good cause to believe that it will have jurisdiction over Defendants because they have purposefully availed themselves of the privilege of doing business in Georgia by infecting, controlling, communicating through, and stealing data from victims and victim computers located throughout the State.

Microsoft owns the registered trademarks "Microsoft," "Windows," and "Edge" and uses these marks in connection with its services, software, and products.

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”). Microsoft owns the registered copyrights in the Windows 8 SDK, Reg. No. TX-8-888-365 (Copyrighted Work). Microsoft’s Copyrighted Work is an original, creative work and copyrightable subject matter under the laws of the United States.

There is good cause to believe that Defendants have engaged in and are likely to engage in future acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the Copyright Act (17 U.S.C. §§ 101 et seq.); the Lanham Act (15 U.S.C. §§ 1114 et seq.); and the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962).

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 law. This harm will be suffered by Microsoft, victims whose computers are infected with Lumma malware, financial institutions who are victimized by Defendants use of stolen credentials to commit financial crimes, and the public at large.

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 infrastructure used to distribute, control, and operate the Lumma malware and computers infected with Lumma malware.

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 infrastructure identified in Appendices 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.

There is good cause to believe that 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) and 1125(c), 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.

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.

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).

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.

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)

transmission by e-mail to abuse contacts for service providers used by Defendants to operate their Lumma infrastructure; (2) publication on publicly accessible websites and/or internet locations known to be visited by Defendants.

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

NOW THEREFORE, IT IS HEREBY ORDERED that Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from:

1. Reproducing, distributing, creating derivative works of, or using unauthorized versions of Microsoft's software;
2. Using without authorization the "Microsoft," "Windows," and "Edge" trademarks;
3. Deploying, installing, executing, or copying malware, computer contaminants, malicious code, or unauthorized software on third party computers;
4. Using infected victims' computers to send commands and instructions to the infected computing device to control it surreptitiously and deliver malware that enables Defendants to take control of the victim's computer or to use such

computers to receive, transmit, or send commands from Lumma malware and associated infrastructure and services; and,

5. Distributing, operating, or using Lumma Malware for purposes of obtaining third party data without authorization.

IT IS FURTHER ORDERED, pursuant to the All Writs Act, with respect to any of the infrastructure set forth in Appendix A to this Order, the owners and/or operator of such infrastructure with a presence in the United States shall take reasonable best efforts to implement the following actions:

6. 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 domains identified in Appendix A;
7. 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 domains identified in Appendix A, by Defendants or Defendants' representatives or resellers, except as explicitly provided for in this Order;
8. Completely disable the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with Defendants' use of the domains 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;

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

10. 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.

11. 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;

12. Not enable, and shall take all reasonable steps to prevent, any circumvention of this order by Defendants or Defendants' representatives associated with the domains including without limited to enabling, facilitating, and/or allowing Defendants or Defendants' representatives or resellers to rent, lease, purchase, or otherwise obtain domains associated with implicated services;

13. Preserve, retain and produce to Plaintiffs all documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling the domains 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;
14. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order; and
15. Completely preserve any computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with the domains set forth in Appendix A, and preserve all evidence of any kind related to the content, data, software or accounts associated with such domains and such computer hardware, such that such evidence of Defendants' unlawful activities is preserved.
16. 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 of record in this action.

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 with a presence in the United States shall take or cause to be taken the following actions:

17. Within three (3) business days of receipt of this Order, or as soon as practicable, 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, or as soon as reasonably practicable, 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.

18. 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;

19. The domain registries shall take reasonable steps to work with Microsoft to ensure the transfer of the domains 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;

20. The WHOIS registrant, administrative, billing and technical contact and identifying information should provide such information as may be specified by Microsoft:

21. Prevent transfer, modification or deletion of the domains by Defendants and prevent transfer or control of the domain to the account of any party other than Microsoft;

22. 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 ISPs and as agreed to by Defendants in their agreements with ISPs, and (4) publishing notice on a publicly available Internet websites.

With respect to any registrars, registries, or infrastructure providers associated with the domains listed in Appendix A that do not have a presence in the U.S. or are not otherwise subject to the Court' jurisdiction, receipt of this Order shall constitute notice that their infrastructure and/or services are being used by Defendants, and voluntary compliance with the provisions of this order is requested.

IT IS FURTHER ORDERED, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before this Court within fourteen days from the date of execution of this order, to show cause, if there is any, why this 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's bond in the amount of \$25,000 paid into the Court registry as part of the case *Microsoft Corp. v. Does 1-10*, No. 1:25-CV-2695-MHC (N.D. Ga. May 15, 2025) ("*Lumma P*") at Dkt. Entry dated 6/12/2025 (receipt #100019912) shall also be held as security in this case.

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.

Dated: November 17, 2025.



U.S. District Court Judge

APPENDIX A

adsay[.]xyz	conbjao[.]qpon	flirtn[.]lol
agnioysz[.]xyz	cotswmr[.]pics	fritron[.]xyz
antiaix[.]qpon	countrnncn[.]xyz	garexqz[.]xyz
anticlk[.]qpon	crimod[.]xyz	geczs[.]xyz
antvu[.]xyz	crowfza[.]xyz	genhqq[.]xyz
aryxnw[.]xyz	dalocoz[.]bet	genusie[.]xyz
assixny[.]xyz	damagex[.]qpon	genuysf[.]bet
atomihc[.]xyz	danglaz[.]lol	glibtof[.]qpon
beyxm[.]xyz	denimmi[.]qpon	guerp[.]xyz
blolln[.]xyz	detru[.]xyz	harmrvw[.]xyz
blotzm[.]xyz	digitbasket[.]com	herwtx[.]xyz
bokcgjf[.]xyz	dogcded[.]bet	hfteozo[.]qpon
bowoqur[.]xyz	dubznetwork[.]com	hickcsp[.]xyz
boxmc[.]xyz	easybqy[.]qpon	hyduwkvd[.]forum
butaqud[.]xyz	echimdi[.]xyz	ideofvb[.]bet
callbacywo[.]xyz	eleccqt[.]bet	immkay[.]xyz
canpnh[.]xyz	enthrqe[.]bet	inflvy[.]xyz
capitam[.]qpon	ethnugm[.]xyz	islamil[.]bet
catachq[.]xyz	excesso[.]qpon	jambzkb[.]qpon
censukpy[.]xyz	exodhr[.]xyz	jocosoj[.]pics
clafvom[.]qpon	facilin[.]qpon	kennetk[.]bet
clirujf[.]xyz	falsapa[.]qpon	kiddykk[.]xyz
coedxz[.]xyz	fecymm[.]xyz	kinwlyo[.]xyz
cojcx[.]xyz	ferzja[.]xyz	kuwtpt[.]xyz
commgxm[.]qpon	fetaokt[.]xyz	lactoxn[.]bet

lakxd[.]xyz	olzoxo[.]xyz	shawq[.]xyz
laputau[.]qpon	opalxrr[.]xyz	shfsz[.]xyz
leasebu[.]bet	openlkn[.]bet	siplv[.]xyz
leftlam[.]xyz	orienderi[.]com	sldnys[.]xyz
lexenorfl[.]org	orienlc[.]bet	splizl[.]xyz
lifyg[.]xyz	permanz[.]qpon	stacdqi[.]xyz
lixkyf[.]xyz	persrbj[.]qpon	starexs[.]bet
markwbp[.]xyz	phoenix-brands[.]dev	stisfmye[.]xyz
maroui[.]xyz	physicianuseptides[.]	strankl[.]xyz
marvelvod[.]com	com	streamin[.]style
masor[.]xyz	pictuqyr[.]qpon	strinth[.]xyz
maszgn[.]club	polytgh[.]bet	subtehi[.]bet
matkdpy[.]xyz	portldu[.]xyz	sunssek[.]xyz
mflqsm[.]xyz	proscns[.]bet	swejog[.]xyz
mindhlo[.]qpon	proxgn[.]xyz	swydug[.]xyz
mindlevqtg[.]xyz	pyrolqi[.]xyz	thicew[.]xyz
mocadia[.]com	pyscalp[.]com	threahg[.]qpon
monbd[.]xyz	quailnf[.]xyz	thumse[.]xyz
monxxb[.]xyz	rabqjz[.]xyz	thuyrxi[.]xyz
myxokgc[.]xyz	ravishl[.]qpon	tilmx[.]xyz
negqjcj[.]xyz	ribbomv[.]xyz	totplh[.]xyz
neticex[.]qpon	roomysc[.]bet	transzw[.]xyz
norcgdu[.]xyz	scallok[.]pics	trichcd[.]bet
nowqx[.]xyz	scapqep[.]club	triobm[.]xyz
nudismh[.]qpon	schrvk[.]xyz	turrqql[.]bet
oblieg[.]xyz	setbnhy[.]bet	twiory[.]xyz
octanzn[.]bet	shaqgn[.]xyz	uncombsguq[.]xyz

unimzfs[.]qpon	solemfk[.]courses
unlfee[.]xyz	stevedw[.]pics
unsuxvxb[.]qpon	strisef[.]mom
utvp1[.]net	stronpn[.]courses
voando26[.]com	suspeter[.]lat
wojbi[.]xyz	teered[.]locker
xurekodip[.]com	throjvy[.]locker
youngnu[.]xyz	upstreu[.]lat
zairez[.]bet	asceniz[.]shop
zwiirl[.]xyz	cannujv[.]shop
bluescm[.]courses	carptrvo[.]shop
chuza[.]locker	dropphef[.]shop
citropt[.]pics	fissiklo[.]shop
czarpve[.]mom	incocrrm[.]shop
fatbaem[.]courses	jocospt[.]shop
hermoae[.]courses	lachcnf[.]shop
holdonz[.]pics	mannewd[.]shop
indef[.]locker	rhusdniw[.]shop
lethali[.]mom	scombxu[.]shop
meeukdt[.]locker	sirtpwv[.]shop
naturah[.]lat	subdvivw[.]shop
nobles[.]locker	sulphuc[.]shop
organbq[.]courses	unapjjh[.]shop
pitchz[.]locker	vitambio[.]shop
retrosa[.]pics	wasxhawg[.]shop
rightea[.]pics	misdgxr[.]shop
rollupf[.]pics	whinmap[.]shop