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

MICROSOFT CORPORATION, Plaintiff, v. DOES 1-10, Defendants.	Case No. 1:25-cv-02695-MHC

SUPPLEMENTAL BRIEF IN SUPPORT OF REQUEST FOR PRELIMINARY INJUNCTION

INTRODUCTION

This case is a civil action by Microsoft against the operators of a malware network and marketplace designed to distribute, control, and monetize the most widely distributed data-stealing malware family in the world, commonly known as the Lumma, LummaStealer, or LummaC2 malware ("Lumma"). On May 15, 2025, the Court issued a Temporary Restraining Order and Order to Show Cause ("TRO") enjoining Defendants from continuing their unlawful conduct and directing the seizure of certain internet domains used by Defendants to carry out their scheme and ordering Defendants to show cause why a Preliminary Injunction should not issue. Dkt. 15. Also on May 15, the Court authorized alternative service

of process on Defendants pursuant to Fed. R. Civ. P. 4(f)(3). Dkt. 16. On May 29, 2025, the Court subsequently extended the TRO for an additional fourteen days for good cause shown. Dkt. 34.

The Court's orders have been effective, resulting in significant disruption of Defendants' malicious Lumma marketplace infrastructure and providing actual notice to Defendants of the TRO, this action, and the Court's orders. *See* Declaration of Derek Richardson (dated June 10, 2025) ("Richardson Supp. Decl.") ¶¶ 4-6. Despite having notice of the TRO, this action, and the Court's orders – including because of Microsoft's notices displayed to Defendants at the seized domains and because of national and international news coverage of the Lumma takedown efforts (*see id.* ¶5-13, Exs. 2-7), no Defendant has responded to the Court's order to show cause or otherwise appeared in the case. Nor has any Defendant responded to multiple emails from Microsoft's counsel providing further notice of this action.

Instead, Defendants responded to Microsoft's seizure of U.S.-based domains under the Court's TRO by attempting to circumvent the TRO by moving certain infrastructure to ISPs located outside of the U.S. and by attempting to continue to operate their scheme today, albeit with significantly diminished capacity. *See id.* ¶5, 7 & Ex. 1. The ringleader of Defendants scheme also took to social media in hopes of reassuring Defendants' customers that distribution and monetization of

the Lumma malware will continue notwithstanding efforts by Microsoft and various domestic and foreign law enforcement agencies. *See id.* ¶7.

Accordingly, a preliminary injunction is warranted to prevent Defendants from regaining control over the malicious domains seized under the TRO.

FACTUAL BACKGROUND

As set forth in further detail in Microsoft's TRO papers, Defendants are associated with creating, distributing, operating, and selling Lumma and associated services and are participants in the conduct of a malware-as-a-service enterprise referred to in Microsoft's Complaint as the Lumma Enterprise. Dkt. 5-4, Declaration of Derek Richardson (dated May 14, 2025), ¶¶ 4-11. In general, the Luma Enterprise is characterized by Defendants' collective efforts to use social engineering techniques designed to trick users into infecting their computers with Lumma malware, to control infected computers through command and control ("C2") infrastructure, and using infected computers and C2 infrastructure to steal data and monetize Lumma-related services in furtherance of financial crimes. *Id.* ¶¶ 21-38. Many of these C2 domains are hardcoded into the Lumma malware itself, while other C2 domains have been provided dynamically through Telegram and Steam Accounts. Dkt. 5-2, Aronov Declaration (dated May 13, 2025), ¶6.

The TRO allowed Microsoft to seize certain internet domains used by Defendants as communication nodes for Lumma C2 servers. Upon issuance of the

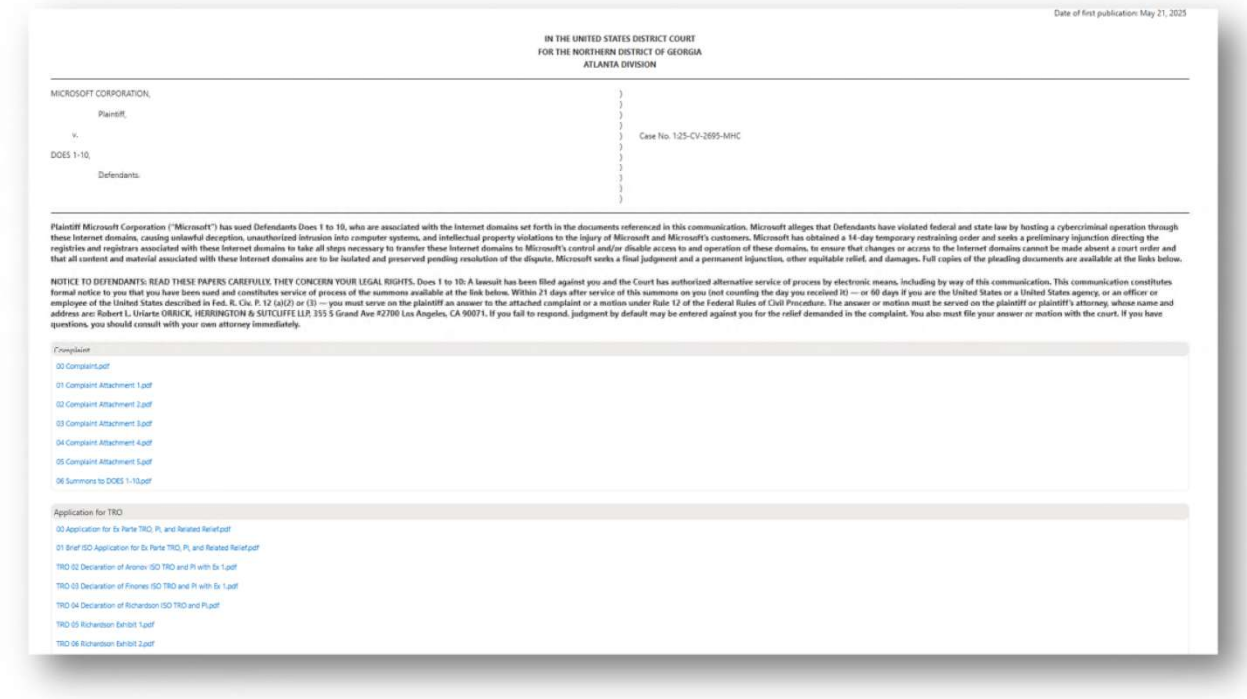
Court's TRO, Microsoft commenced efforts to execute the TRO by notifying relevant third-party Internet Service Providers. *See* Richardson Supp. Decl. ¶3. After C2 domains were redirected from Defendants C2 servers to a Microsoft sinkhole domain, visitors to C2 domains would have encountered a notice banner notifying them of this case and providing a link to access all case documents, as show in Figure 1 below:

Figure 1

Richardson Supp. Decl. ¶ 6. The banner in Figure 1 provides a link to the URL aka.ms/dcuPleadings which in turn provides a link to the "documents about the Lumma botnet lawsuit" at https://www.noticeofpleadings.net/lumma/index.html,

which provides access to all documents filed in this case, as shown in Figure 2 below. *Id*.

Figure 2



Date of first publication: May 21, 2025

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

MICROSOFT CORPORATION,
Plaintiff,
v.
DOES 1-10,
Defendants.

Case No. 1:25-CV-2695-MHC

Plaintiff Microsoft Corporation ("Microsoft") has sued Defendants Does 1 to 10, who are associated with the Internet domains set forth in the documents referenced in this communication. Microsoft alleges that Defendants have violated federal and state law by hosting a cybercriminal operation through these Internet domains, causing unlawful deception, unauthorized intrusion into computer systems, and intellectual property violations to the injury of Microsoft and Microsoft's customers. Microsoft has obtained a 14-day temporary restraining order and seeks a preliminary injunction directing the registries and registrars associated with these Internet domains to take all steps necessary to transfer these Internet domains to Microsoft's control and/or disable access to and operation of these domains, to ensure that changes or access to the Internet domains cannot be made absent a court order and that all content and material associated with these Internet domains are to be isolated and preserved pending resolution of the dispute. Microsoft seeks a final judgment and a permanent injunction, other equitable relief, and damages. Full copies of the pleading documents are available at the links below.

NOTICE TO DEFENDANTS: READ THESE PAPERS CAREFULLY. THEY CONCERN YOUR LEGAL RIGHTS. Does 1 to 10: A lawsuit has been filed against you and the Court has authorized alternative service of process by electronic means, including by way of this communication. This communication constitutes formal notice to you that you have been sued and constitutes service of process of the summons available at the link below. Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are: Robert L. Uriarte ORRICK, HERRINGTON & SUTCLIFFE LLP, 355 S Grand Ave #2700 Los Angeles, CA 90071. If you fail to respond, judgment by default may be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court. If you have questions, you should consult with your own attorney immediately.

Complaint
00 Complaint.pdf
01 Complaint Attachment 1.pdf
02 Complaint Attachment 2.pdf
03 Complaint Attachment 3.pdf
04 Complaint Attachment 4.pdf
05 Complaint Attachment 5.pdf
06 Summons to DOES 1-10.pdf

Application for TRO
00 Application for Ex Parte TRO, PI, and Related Relief.pdf
01 Brief ISO Application for Ex Parte TRO, PI, and Related Relief.pdf
TRO 02 Declaration of Aronov ISO TRO and PI with Ex 1.pdf
TRO 03 Declaration of Finones ISO TRO and PI with Ex 1.pdf
TRO 04 Declaration of Richardson ISO TRO and PI.pdf
TRO 05 Richardson Exhibit 1.pdf
TRO 06 Richardson Exhibit 2.pdf

Concurrently with Microsoft's execution of the TRO, law enforcement agencies in the United States and Europe undertook their own actions to disrupt Lumma malware marketplace infrastructure in the U.S. and abroad. Richardson Supp. Decl. ¶3-4. Defendants attempted to circumvent these efforts by moving certain infrastructure to ISPs located outside of the U.S. *Id*. ¶5. Defendants also undertook to reassure Lumma marketplace participants that despite efforts to disable Defendants malicious infrastructure, Defendants remain operational via infrastructure that is beyond the reach of U.S. law. *See id*. ¶7 & Ex. 1. Microsoft

believes that DOE 1 aka "Shamel" caused publication of a statement on the "X" social media platform which stated that "almost 2,500 domains were really seized from us [as] is evidenced by the press release of Europol." *Id.* Shamel continued "the FBI itself [] did not seize our server… because it is located in a country where they definitely cannot seize it," that subsequent to May 16, 2025 "we quickly restored functionality" but thereafter "the server was formatted again along with the backup server," and "they intercepted our domain[s] ... [to] collect[]" information about and attempt to shutdown Lumma. *Id.*

ARGUMENT

"The same standard applies to a request for a TRO and a request for preliminary injunction." *Interra Int'l, LLC v. Al Khafaji*, No. 16-cv-1523-MHC, 2016 WL 10262650, at *3 (N.D. Ga. July 15, 2016) (citing *Ingram v. Ault*, 50 F.3d 898, 900 (11th Cir. 1995)). "Parties seeking a preliminary injunction must demonstrate that (1) they are likely to succeed on the merits, (2) they are likely to suffer irreparable harm, (3) the balance of hardships tips in their favor, and (4) the injunction is in the public interest." *Winter v. Natural Res. Def. Council, Inc*., 555 U.S. 7, 20 (2008). The Court considered these same factors in issuing the TRO and there is "no reason to disturb" those findings, particularly in view of Defendants' failure to respond to the Court's Order to Show Cause. *See Clearone Advantage, LLC v. Kersen*, 713 F. Supp. 3d 86, 87-88 (D. Md. 2024) (citing

Glaxosmithkline, LLC v. Brooks, 2022 WL 2916170, at *2 (D. Md. July 25, 2022) for the proposition that it "may be appropriate to convert a TRO into a preliminary injunction as a result of a defendant's failure to defend and/or failure to appear" and 11A Charles Alan Wright & Arthur R. Miller, Federal Practice and Procedure § 2949 (3d ed. 2023) (explaining that an evidentiary hearing on a preliminary injunction request is not required when there is no genuine controversy)); *Roche Diagnostics Corp. v. Priority Healthcare Corp.*, No. 2:18-CV-01479-KOB-HNJ, 2019 U.S. Dist. LEXIS 193454, at *5 (N.D. Ala. Nov. 7, 2019) (converting TRO to preliminary injunction based on "many of the same facts[] featured in the temporary restraining order.").

All four injunction factors continue to weigh in Microsoft's favor.

Likelihood of Success. Microsoft is likely to succeed on the merits of its CFAA, Lanham Act, Copyright, and RICO claims for the same reasons that supported issuance of the TRO. Microsoft is likely to prevail on its CFAA claim because Defendants have in the past—and continue today—to access infected Windows computers without authorization. *See, e.g., Microsoft Corp. v. Does 1-51*, No. 1:17-CV-4566, 2017 WL 10087886 at *4 (N.D. Ga. Nov. 17, 2017) (finding Microsoft's and Microsoft's customers computers to be protected computers); *Volk v. Zeanah*, No. 608CV094, 2010 U.S. Dist. LEXIS 5621, at *4 (S.D. Ga. Jan. 25, 2010) ("The CFAA is meant to reduce hacking of computer

systems/networks"); *Schwartz v. ADP, Inc*., No. 2:21-cv-283-SPC-MRM, 2021 U.S. Dist. LEXIS 231613, at *3 (M.D. Fla. Dec. 3, 2021) ("The CFAA punishes computer hacking").

Defendants also continue to misleadingly user Microsoft's trademarks to trick users into using corrupted versions of Windows, which violates the Lanham Act. *See, e.g.*, *Garden & Gun, LLC v. Twodalgals, LLC*, 2008 U.S. Dist. LEXIS 79982 (W.D.N.C. 2008) (granting preliminary injunction against misleading use of trademarks under Section 1125(a)); *Am. Online v. IMS*, 24 F. Supp. 2d 548, 551-552 (E.D. Va. 1998) (misuse of trademark in e-mail headers violated §1125(a); also constituted trademark "dilution" under §1125(c)); *Brookfield Commc'ns.,* 174 F. 3d at 1066-67 (entering preliminary injunction under Lanham Act §1125(a) for infringement of trademark in software and website code); *Microsoft Corp. v. Doe*, 2021 U.S. Dist. LEXIS 101862, at *13-14 (E.D.N.Y. May 28, 2021) ("[malware] does not intend to just compete with the Windows operating system, it intends to hide itself within the system to take over and replace it without the user's knowledge," and "[i]n the eyes of the user, [malware] becomes Microsoft, but it is not Microsoft at all. Nor is the user aware that [malware] is manipulating their devices to commit cybercrimes.").

Defendants also continue to infringe on Microsoft's copyrights by misusing hundreds of lines of API code. *See, e.g.*, *Microsoft Corp. v. Does*, 2021 U.S. Dist.

LEXIS 258143, at *9 (E.D. Va. Aug. 12, 2021); ***Oracle Am., Inc. v. Google Inc.***, 750 F.3d 1339, 1358 (Fed. Cir. 2014) (discussing copyright protection for APIs).

The continuing threat posed by Defendants also bolsters Microsoft's likelihood of success on its RICO claim. *See, e.g.*, *Cisneros v. Petland, Inc.*, 972 F.3d 1204, 1211 (11th Cir. 2020) (discussing elements, including pattern element); *United States v. Carson*, 52 F.3d 1173, 1181-82 (2d Cir. 1995) ("the jurisdictional powers in § 1964(a) serve the goal of foreclosing future violations," and "the equitable relief under RICO is intended to be broad enough to do all that is necessary"). Defendants continue to carry out their criminal enterprise, engaging in wire fraud and criminal violations of U.S. intellectual property laws for financial gain—the fact that Defendants are undeterred by Microsoft's civil case and criminal actions instituted by law enforcement officials underscores Defendants criminality and the ongoing nature of their unlawful enterprise. *See, e.g., United States v. 113 Virtual Currency Accounts*, Civil Action No. 20-606, 2020 U.S. Dist. LEXIS 142015, at *2 (D.D.C. Aug. 4, 2020) ("the hacking and theft of virtual currencies in violation of 18 U.S.C. § 1343"); *Synopsys, Inc. v. Ubiquiti Networks*, Inc., No. 17-cv-00561-WHO, 2017 U.S. Dist. LEXIS 130070, at *38 (N.D. Cal. Aug. 15, 2017) ("using the counterfeit access device…in order to obtain money, goods, services, or any other thing of value" violates 1029).

Irreparable Harm. The harms that supported issuance of the TRO are ongoing, although they have abated in part thanks to the efforts of Microsoft, its private partners, and law enforcement agencies. Nevertheless, the threat of additional harm if no injunction issues remains, particularly given Defendants' efforts to circumvent Microsoft's domain seizures by moving malicious infrastructure offshore and continued marketing and operation of the Lumma malware marketplace bolster Microsoft's case for preliminary injunctive relief. *See, e.g., Int'l Labor Mgmt. Corp. v. Perez,* 2014 U.S. Dist. LEXIS 57803, 35 (M.D.N.C. Apr. 25, 2014) (damage to "reputation and loss of goodwill constitutes irreparable harm for purposes of injunctive relief"); *Nabisco Brands, Inc. v. Conusa Corp.,* 722 F. Supp. 1287, 1290 (M.D.N.C. 1989) ("In the context of a trademark infringement dispute, several courts have held that where likelihood of confusion is established likelihood of success on the merits as well as risk of irreparable harm follow."); *Dynamic Diagnostics, LLC v. Wilken*, No. 2:24-cv-310-RAH-SMD, 2024 U.S. Dist. LEXIS 120931, at *10 (M.D. Ala. July 10, 2024) ("evidence showing that Defendant has continued to compete with Plaintiff and solicit Plaintiff's clients despite knowing that this Court has issued a temporary restraining order prohibiting him from doing so" supported preliminary injunction).

Balance of Equities. The balance of equities remain entirely in Microsoft's favor. The fact that Defendants have actively circumvented the TRO and boasted about being beyond the reach of U.S. law underscores the equity of a preliminary injunction. *See, e.g., Dynamic Diagnostics*, 2024 U.S. Dist. LEXIS 120931 at *10; *see also Airways, Inc. v. US Airline Pilots Ass'n*, 813 F. Supp. 2d 710, 736 (W.D.N.C.2011); *Pesch v. First City Bank of Dallas*, 637 F. Supp. 1539, 1543 (N.D. Tex. 1986) (balance of hardships clearly favors injunction where enjoined activity is illegal).

Public Interest. The public has a strong interest in enforcing laws like the CFAA, RICO Act, Copyright Act, and Lanham Act. *See, e.g., ProFitness Phys. Therapy Ctr. v. Pro-Fit Ortho. And Sports Phys. Therapy P.*C., 314 F.3d 62, 68 (2d Cir. 2002) (finding a "strong public interesting in preventing public confusion"); *BSN Med., Inc. v. Art Witkowski*, 2008 U.S. Dist. LEXIS 95338, 10 (W.D.N.C. Nov. 21, 2008) (same); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, 32 (E.D. Va. Jan. 6, 2014) (CFAA); *Amazon.com, Inc. v. WDC Holdings LLC*, Civil Action No. 1:20-cv-484, 2020 U.S. Dist. LEXIS 134555, at *31 (E.D. Va. July 28, 2020) (RICO). The public's interest is even stronger today than it was when the TRO issued, as it is clear that Defendants intend to continue victimizing the public despite court orders and law enforcement action designed to protect the public. Such bad faith conduct supports an injunction. *E.g., Mey v. Pintas*, Civil Action

No. 5:24-CV-55, 2024 U.S. Dist. LEXIS 99273, at *13 (N.D.W. Va. May 17, 2024) (bad faith conduct supported injunction); *Walsh v. Med. Staffing of Am., LLC*, 2023 U.S. Dist. LEXIS 203645, at *14 (E.D. Va. Sep. 7, 2023 (Similar).

CONCLUSION

For the foregoing reasons, Microsoft respectfully requests issuance of a preliminary injunction. A proposed preliminary injunction is attached.

Dated: June 11, 2025

Respectfully submitted,

/s/ Joshua D. Curry
Joshua D. Curry

Joshua D. Curry (Georgia Bar No. 117378)
Jonathan D. Goins (Georgia Bar No. 738593)
LEWIS BRISBOIS BISGAARD & SMITH LLP
600 Peachtree Street NE, Suite 4700
Atlanta, GA 30308
Tel: 404.348.8585
Fax: 404.467.8845
josh.curry@lewisbrisbois.com
jonathan.goins@lewisbrisbois.com

ROBERT L. URIARTE (*Pro Hac Vice*)
ruriarte@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
355 S. Grand Ave.
Ste. 2700
Los Angeles, CA 90017
Telephone: + 1 213 629 2020
Facsimile: + 1 213 612 2499

JACOB M. HEATH (*Pro Hac Vice*)
jheath@orrick.com
ANA M. MENDEZ-VILLAMIL (*Pro Hac Vice*)
amendez-villamil@orrick.com

ORRICK, HERRINGTON & SUTCLIFFE LLP
The Orrick Building
405 Howard Street
San Francisco, CA 94105
Telephone: + 1 415 773 5700
Facsimile: + 1 415 773 5759

LAUREN BARON (*Pro Hac Vice*)
lbaron@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, NY 10019
Telephone: + 1 212 506 5000
Facsimile: + 1 212 506 5151

Of Counsel:

RICHARD BOSCOVICH
rbosco@microsoft.com
MICROSOFT CORPORATION
Microsoft Redwest Building C
5600 148th Ave NE
Redmond, Washington 98052
Telephone: +1 425 704 0867
Facsimile: +1 425 706 7329

Attorneys for Plaintiff
MICROSOFT CORPORATION

CERTIFICATION OF COMPLIANCE

Pursuant to L.R. 7.1(D), N.D. Ga., counsel for Plaintiff hereby certifies that this Motion has been prepared with one of the font and point selections approved by the Court in L.R. 5.1, N.D. Ga.

Dated: June 11, 2025 */s/ Joshua D. Curry*

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on the date indicated below the foregoing document with any attachments was filed using the Court's CM/ECF System, which caused counsel of record for the parties to be served by electronic mail, as more fully reflected on the notice of electronic filing.

Dated: June 11, 2025 */s/ Joshua D. Curry*