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

MICROSOFT CORPORATION, a Washington corporation, FS-ISAC, INC., a Delaware Corporation, HEALTH-ISAC, INC., a Florida corporation, Plaintiffs, v. DENIS MALIKOV, and JOHN DOES 1-7, Defendants.	)	Civil Action No: 1:22-cv-1328-MHC

BRIEF IN SUPPORT OF PLAINTIFFS' MOTION FOR DEFAULT JUDGMENT AND PERMANENT INJUNCTION

I. INTRODUCTION

Plaintiffs Microsoft Corporation ("Microsoft"), FS-ISAC, Inc. ("FS-ISAC"), and HEALTH-ISAC, Inc. ("H-ISAC") (collectively "Plaintiffs") seek a default judgment and permanent injunction to prevent Defendant Denis Malikov and John Does 1-7 (collectively "Defendants") from continuing to use the malicious computer network infrastructure known as a "botnet" to operate an Internet-based cybercriminal operation to spread malicious software ("malware") knowns as "ZLoader". As set forth in Plaintiffs' pleadings and the Court's previous orders, the ZLoader malware is spread through compromised Internet domains used in

connection with Defendants' cybercrime operation to infect end-user computers with malware and steal high-value, confidential and sensitive information from those end-user computers. Prior to issuance of this Court's Temporary Restraining Order and Preliminary Injunction (Dkts. 27, 41),

Defendants propagated and controlled the ZLoader malware through Internet domains used to relay instructions to infected computers. In particular, Defendants propagated and controlled the malicious infrastructure using a domain that makes deceptive use of Plaintiffs' trademarks and brands. Plaintiff now seeks to bring this case to final conclusion by way of a permanent injunction that will prevent Defendants from continuing to propagate the ZLoader malware or retaking control of the operation through abuse of Plaintiffs' trademarks and brands, once this case is closed. Plaintiffs request an injunction (1) prohibiting Defendants from operating the infrastructure used to propagate ZLoader malware and (2) permanently transferring ownership to Microsoft of known malicious domains identified in the Court's prior injunction order that are used in connection with the command and control ("C2") servers to communicate with the ZLoader malware on infected devices.

This injunctive relief is required to prevent further harm to Plaintiffs and the general public that would be caused if Defendants are able to continue to propagate

and retake control of the infrastructure. A permanent injunction is the only way to afford relief and abate future harm in this case. This is particularly the case, given that, in the absence of such relief, the existing C2 domains would revert to the Defendants.

Plaintiffs duly served Defendants with the Complaint, Summons, and all pleadings and orders of the Court in this action in a manner consistent with Due Process and this Court's instructions. Plaintiffs served Defendants on April 14, 2022 and thereafter, by e-mail and publication at the website http://www.noticeofpleadings.com/zloader. Defendants failed to respond and the Clerk of the Court entered default on October 4, 2022. The factual allegations in the Complaint and the record in the case establish the elements of each of Plaintiffs' claims and also establishes the need for the requested injunctive relief.

II. FACTUAL BACKGROUND

This action arises out of violations of federal and state law caused by Defendants' operation of a harmful cybercriminal operation carried out through Internet domains used to distribute and control the ZLoader malware.

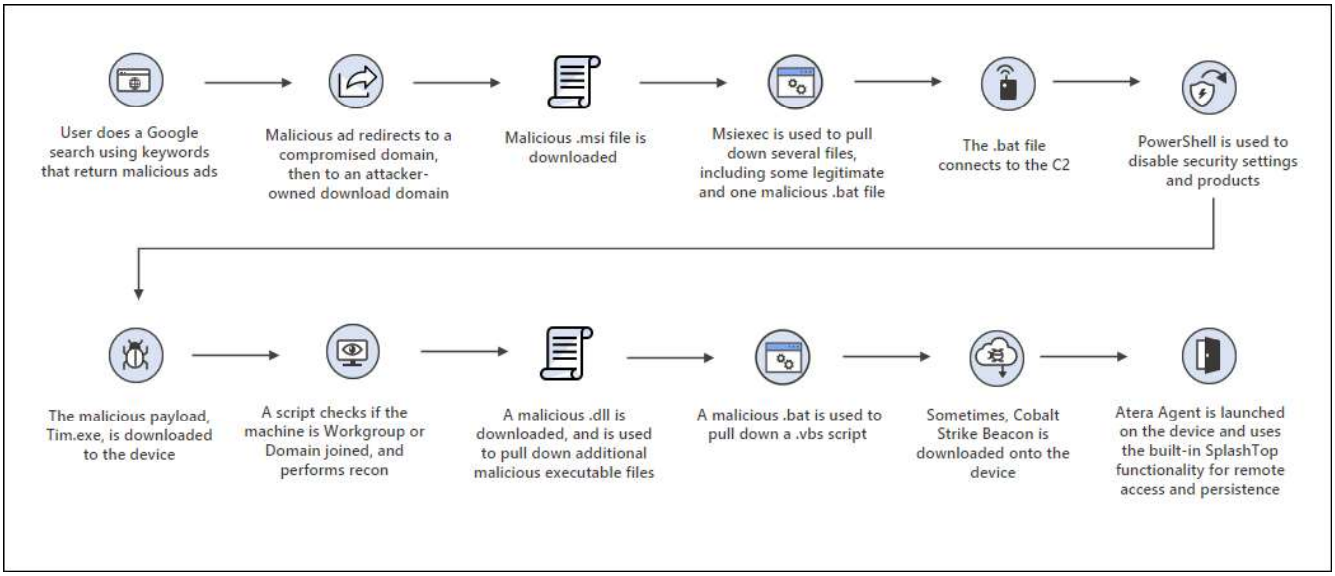
Overview of ZLoader

ZLoader is a prolific and globally diverse financial theft and malware distribution botnet. The ZLoader botnet has infected over 200,000 computing

devices, of the type commonly found in businesses, living rooms, schools, libraries, and Internet cafes around the world. ZLoader specializes in distributing ransomware, and infecting end user computers in order to steal financial account credentials, funds, and personal information. Dkt. 1 at ¶ 29.

The Defendants have engaged in a pattern of racketeering activity through an associated-in-fact enterprise with the purpose of creating, distributing, and monetizing the ZLoader botnet, and associated ransomware and malware distribution tools (the "ZLoader Criminal Enterprise"). The ZLoader Criminal Enterprise targets Plaintiffs' customers and members, including end users who use Microsoft's operating system, financial institutions whose customers are stolen from, and health care institutions who are targeted by ransomware. ZLoader malware, constituting the ZLoader botnet, is disseminated via malicious advertisements, exploits, spam email and spearphishing campaigns, among other methods. The spam email and spearphishing campaigns send unsolicited messages that deceive targeted victims into downloading the ZLoader malware from malicious websites or through malicious attachments, such as those designed to look like legitimate Microsoft Word or Excel files. Once the ZLoader Criminal Enterprise caused enough computers to be infected with the ZLoader malware, the Defendants, constituting the ZLoader Criminal Enterprise, built a scaled ZLoader botnet through

which they carry out their illegal acts. *Id.* at ¶ 30. The ZLoader Criminal Enterprise uses the ZLoader botnet to install malware, allowing the defendants to steal financial, health, and other personal information from the owners of the infected computers surreptitiously, without the user being aware that their computer has been compromised. *Id.* at ¶ 31. The ZLoader Criminal Enterprise targets financial institutions that are members of FS-ISAC through their distribution and use of financial theft malware. The ZLoader Criminal Enterprise targets health care institutions that are members of H-ISAC through their distribution and use of ransomware. Dkt. 1 at ¶ 31. Plaintiffs have seen distribution of ZLoader malware to infect victim devices through the leveraging of online advertisement platforms. For example, while the ZLoader Criminal Enterprise previously relied upon phishing emails, it now leverages online ad platforms. Specifically, the ZLoader Criminal Enterprise purchases online ads that direct victims to websites hosting malware posing as legitimate installers. *Id.* at ¶ 35. The following chart demonstrates the step-by-step method that ZLoader uses to infect victims' devices:



Each ZLoader C2 server domain, like any other domain, is managed by a registry service, which facilitates association of the domain with an IP address . The ZLoader domains at issue in the present proceedings are managed by the registry services listed in **Appendix A** to the Complaint. *Id.* at ¶ 45.

Malware infections tarnish the reputation of Plaintiffs and their products and services, because consumers incorrectly attribute the harm caused by ZLoader to Plaintiffs' products and services. *Id.* at ¶¶ 102; 179. This creates a serious risk that customers may abandon Plaintiffs products and services, and once this occurs, there are significant challenges to winning the customers back. *Id.*

The Court's Injunction, Defendants' Disregard of the Injunction, and Defendants' Continued Harmful Activities Through the Course of This Case

On April 8, 2022, the Court entered a TRO that disabled the ZLoader domains Defendants used to deceive victims and as command and control infrastructure, as discussed above. Dkt. 27. The Court subsequently entered a Preliminary Injunction disabling the same domains on April 26, 2022. Dkt. 41.

In the foregoing injunction order, and consistent with the unrebutted allegations in the Complaint, the Court has made several factual findings and conclusions of law. Among other findings, the Court concluded that:

- The Court has jurisdiction;
- Defendants have used, and are likely to continue to use, domains identified by Plaintiffs throughout this case to operate the infrastructure used to distribute and control the ZLoader malware;
- Defendants have used, and are likely to continue to use, domains containing Plaintiffs' trademarks and brands to deceive victims and operate the infrastructure used to distribute and control the ZLoader malware;
- Defendants' activities concerning the domains has violated or is likely to violate (1) the Computer Fraud and Abuse Act (18 U.S.C. *§* 1030), (2) the Electronic Communications Privacy Act (18 U.S.C. § 2701), (3) the Georgia Computer Systems Protection Act (O.C.G.A. § 16-9-93), (4) the Lanham Act

(15 U.S.C. § 1114 et seq.), (5) the Racketeer Influenced and Corrupt Organizations Act (18 U .S.C. § 1962), (6) conversion and trespass (O.C.G.A. § 51-10-1 et seq.), (7) unjust enrichment, and (8) the All Writs Act (28 U.S.C. § 1651);

- Unless enjoined, Defendants are likely to continue to engage in conduct that violates (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030), (2) the Electronic Communications Privacy Act (18 U.S.C. § 2701), (3) the Georgia Computer Systems Protection Act (O.C.G.A. § 16-9-93), (4) the Lanham Act (15 U.S.C. § 1114 et seq .), (5) the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962), (6) conversion and trespass (O.C.G.A. § 51 -1 0-1 et seq.), (7) unjust enrichment, and (8) the All Writs Act, (28 U.S.C. § 1651);
- Defendants have received notice of the injunction and, despite that fact, are likely to continue to register and use domains containing Plaintiffs' trademarks and brands to deceive victims and control the ZLoader infrastructure;
- Defendants' conduct causes irreparable harm and such irreparable harm will continue unless the domains used by Defendants are disabled and unless

Defendants are subject to an expedited process to disable new malicious domains registered by Defendants as they are put into operation.

Service of Process on Defendants

The Court authorized service by e-mail and publication on April 8, 2022. Dkt. 27. Beginning on April 14, 2022 and repeatedly thereafter, Plaintiffs carried out service of process on Defendants by e-mail to e-mail addresses associate with Defendants' Internet domains and by publication on a public website http://www.noticeofpleadings.com/zloader. Dkt. 27 at pp. 13-14. The time for Defendants to answer or respond to the complaint expired 21 days after services of the summons, yet despite repeated notice and service the Defendants did not respond. Dkt. 44-1 at ¶¶ 2-4. The Clerk of Court entered Defendants' default pursuant to Federal Rules of Civil Procedure 55(a) on October 4, 2022.

III. LEGAL STANDARD

Rule 55 of the Federal Rules of Civil Procedure and O.C.G.A. § 9-l 1-55(a) authorizes the entry of a default judgment when a defendant fails to plead or otherwise defend within the proscribed time period. *See* O.C.G.A. § 9-11-55(a) (providing that a "case shall automatically become in default" if the defendant's answer is not filed within the period allowed by law or within a properly obtained extension of the period); *Wahlv. Mciver*, 773 F.2d 1169, 1174 (11th Cir. 1985). In

turn a court is authorized to enter a default judgment against a properly served defendant who fails to file a timely responsive pleading. *See Sidwell v. Sidwell*, 237 Ga. App. 716, 717, 515 S.E.2d 634, 635 (1999) (the moving party is entitled, as a matter of law, to verdict and judgment by default as if every item and paragraph of its complaint were supported by proper evidence); *Georgia Power Project v. Georgia Power Co.*, 409 F.Supp. 332 (N.D. Ga. 1975); *S.E.C. v. Johnson*, 436 Fed.Appx. 939, 944-45 (enter default against defendant for failing to "appear, answer or otherwise plead to the complaint . . . within the time required by law" under Rule 55(a)); *Arango v. Guzman*, 761 F.2d 1527, 1531 (11th Cir. 1985) (default judgment entered when party failed to appear). Upon default, the well-pled allegations in a complaint as to liability are taken as true. *See Pitts ex rel. Pitts v.Seneca Sports, Inc.*, 321 F.Supp.2d 1353, 1356, 1358 (11th Cir. 2004); *Tyco Fire & Sec., LLC v. Alcocer*, 218 Fed.App'x. 860, 863 (11th Cir. 2007); *see also* Fed. R. Civ. P. 8(b)(6) ("An allegation- other than one relating to the amount of damages-is admitted if a responsive pleading is required and the allegation is not denied ."). Here, the Clerk has entered Defendants' default under Rule 55(a), and Defendants have received notice of same.

Courts may order permanent injunctive relief in conjunction with default judgments. *E.g.*, *Trs. of the Nat'/ Asbestos Workers Pension Fund v. Ideal*

Insulation, Inc., 2011 U.S. Dist. LEXIS 124337, at * 12 (D. Md. Oct. 27, 2011) (collecting cases). Permanent injunctions depriving cybercrime defendants of their malicious infrastructure, on an ongoing basis in the future, have been entered by courts in connection with entry of default judgments. *See America Online v. IMS*, 1998 U. S. Dist. LEXIS 20645 (E.D. Va. Dec. 30, 1998) (Brinkema, J.); *Microsoft Cmp. v. Doe*, 2015 U.S. Dist. LEXIS 109729 (E.D. Va. Aug. 17, 2015) (O'Grady, J.); *Microsoft Corp. v. Doe*, 2015 U.S. Dist. LEXIS 110145 (E.D. Va. July 20, 2015) (Report and Recommendation); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 46951 (E.D. Va. Apr. 2, 2014) (Brinkema, J.); *Microsoft Corp.* v. *Doe*, 2014 U.S. Dist. LEXIS 48398 (E.D. Va. Jan. 6, 201 4) (Report and Recommendation); *see also Microsoft Corp. v. Does*, 2013 U .S. Dist. L EXIS 168237 (W. D.N.C. Nov. 21, 2013).

IV. DISCUSSION

A. DUE PROCESS HAS BEEN SATISFIED

Plaintiff has served the Complaint, Summons, and all orders and pleadings on Defendants using the methods ordered by the Court under Rule 4(f)(3), including service by e-mail and publication. It is well settled that legal notice and service by e-mail, facsimile, mail, and publication satisfies Due Process where these means are reasonably calculated, in light of the circumstances, to put defendants on notice. *See*

e.g., *In re Int'l Telernedia Associates, Inc.*, 245 B .R. 713, 720-21 (N.D. Ga. 2000) (authorizing service by electronic mail under Rule 4(f)(3)); *Black & D ecker Inc. v. King Group Canada*, 2009 WL 10670400, at *3 (N.D. Ga. 2009) (holding that service upon defendants by e-mail is appropriate under Rule 4(f)(3)); *Rio Props., Inc. v. Rio Int'l Interlink*, 284 F.3d 1007, 1014-15 (9th Cir. 2002) (involving Internet-based misconduct; "[Defendant] had neither an office nor a door; it had only a computer terminal. If any method of communication is reasonably calculated to provide [Defendant] with notice, surely it is email"). E-mail service and Internet publication are particularly appropriate here given the nature of Defendants' conduct and use of e-mail as the primary means of communication in connection with establishing and managing the IP addresses and domains used to operate the C2 domains and infrastructure. *See id.*

In this case, the e-mail addresses provided by Defendants to the domain registrars, in the course of obtaining services that support the Defendants' C2 infrastructure, are the most accurate and viable contact information and means of notice and service. Indeed, the physical addressees provided by Defendants to domain registrars and other service providers are false and Defendants' whereabouts are unknown, and are not ascertainable despite the exercise of diligent formal and informal attempts to identify the Defendants, which further supports service by e-

mail and publication. *See In re Int'l Telemedia Associates, Inc.*, 245 B.R. at 720-21; *BP Products North Am., Inc.*, 236 F.R.D. 270, 271 (2006). Moreover, Defendants will expect notice regarding their use of the domain registrars' services to operate their C2 infrastructure by e-mail, as Defendants agreed to such in their agreements with the service providers who provided the domains for Defendants' use. *See Nat'l Equip. Rental, Ltd. v. Szukhent*, 375 U.S. 311 (1964) ("And it is settled that parties to a contract may agree in advance to submit to the jurisdiction of a given court, to permit notice to be served by the opposing party, or even to waive notice altogether.").

Given the circumstances and Plaintiffs' diligent efforts to provide notice to Defendants, Due Process has been satisfied by Plaintiffs' service by publication and multiple e-mail notices.

B. DEFAULT JUDGMENT IS APPROPRIATE

In reviewing motions for default judgment, courts have referred to the following factors: (1) the amount of money involved in the litigation; (2) whether there are material issues of fact in the case needing resolution; (3) whether the case involves issues of great public importance; (4) whether the grounds for the motion for a default judgment are highly technical; (5) whether the party asking for a default judgment has been prejudiced by the non-moving party's actions or omissions; (6)

whether the actions or omissions giving rise to the motion for a default judgment are the result of a good-faith mistake on the part of the non-moving party; (7) whether the actions or omissions giving rise to the motion for a default judgment are the result of excusable neglect on the part of the non-moving party; and (8) whether the grounds offered for the entry of a default judgment are clearly established. *Tweedy*, 611 F. Supp. 2d at 605-606 (citing *Faulknier v. Heritage Financial Corp*., 1991 U.S. Dist. LEXIS 15748 (W.D. Va. May 20, 1991) and 10 C.Wright, A. Miller & M. Kane, Federal Practice and Procedure§§ 2684-85 (1990)). All of the relevant considerations point towards issuance of a default judgment against Defendants.

First, the amount of money at stake weighs in favor of default judgment because Plaintiff is not requesting any monetary relief, and indeed it is not possible for Plaintiff to obtain any meaningful monetary relief under the circumstances. Accordingly, default judgment poses no risk of undue cost, prejudice, or surprise to Defendants.

Second, there are no material facts in dispute. Plaintiff has put forth a strong factual showing supported by expert testimony, forensic evidence, and documentary evidence from researchers who have studied the infrastructure used to propagate the ZLoader malware and its impact on victims. The allegations and evidence in the detailed Complaint and otherwise in the record establish that the Defendants'

conduct in operating the C2 infrastructure used to propagate and control the ZLoader malware violated and are likely in the future to violate (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030), (2) the Electronic Communications Privacy Act (18 U.S.C. § 2701), (3) the Georgia Computer Systems Protection Act (O.C.G.A. § 16-9-93), (4) the Lanham Act (15 U.S.C. *§* 1114 et seq.), (5) the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962), (6) conversion and trespass (O.C.G.A. § 51-10-1 et seq.), (7) unjust enrichment, and (8) the All Writs Act, (28 U.S.C. § 1651).

Third, this case involves a matter of substantial public importance. Defendants are perpetrating serious offenses and civil torts that cause substantial harm to hundreds if not thousands of victims. In addition to the general public interest in abating such harm, the public also has a strong interest in the integrity and enforcement of federal laws designed to deter cybercrime and enhance data security.

Fourth, default here is not merely technical. This is not a situation where Defendants have accidentally missed a deadline by a few days. Nor is default the result of a good faith mistake or excusable neglect. Rather, Defendants have affirmatively chosen not to appear and defend this action, despite ample notice and opportunity to do so. Plaintiff has made extraordinary efforts over the course of many months to ensure that Defendants were provided notice, and the evidence

indicates that Defendants are actually aware of this action, but affirmatively choosing not to appear.

Fifth, Plaintiff and other victims of the ZLoader malware have been prejudiced by the Defendants' actions and omissions. Defendants have refused to make their identities known and have refused to participate in this lawsuit. Defendants' disregard for this Court's process and refusal to communicate have caused Plaintiff to incur significant expense.

Finally, the grounds offered for the entry of a default judgment are clearly established. Plaintiffs application for Default and supporting declaration establish that Defendants have been served. Moreover, the detailed Complaint and the record as a whole establishes Defendants' unlawful conduct and the harm it has caused.

C. Plaintiff Has Adequately Pled Each of its Claims

The Complaint alleges that the Defendants have violated (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030), (2) the Electronic Communications Privacy Act (18 U.S.C. § 2701), (3) the Lanham Act (15 U.S.C. § 1114 et seq. and 15 U.S.C. § 1125(a),(c)), (4) the Georgia Computer Systems Protection Act O.C.G.A. § 16-9-93), (5) the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962(c)-(d), (6) conversion and trespass (O.C.G.A. § 51-10-1 et seq.),

(7) unjust enrichment, and (8) the All Writs Act, (28 U.S.C. § 1651). Each of these claims is adequately pled.

CFAA Claim. The CFAA penalizes a party that: (1) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage, 18 U.S.C. § 1030(a)(5)(C); or (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer, 18 U.S.C. § 1030(a)(2)(C); or (3) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage to a protected computer, 18 U.S.C. § 1030(a)(5)(A); *Andritz v. Southern Maintenance Contractor, LLC*, 626 F.Supp.2d 1264, 1266 (M.D. Ga. 2009). A "protected computer" is a computer "used in interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2). The phrase "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled to obtain or alter." 18 U.S.C. § 1030(e)(6). To prosecute a civil claim under the CF AA, a plaintiff must demonstrate loss or damage in excess of $5,000. 18 U.S.C. § 1030(c)(4)(A)(i)(l). The Complaint alleges that Defendants have surreptitiously accessed protected computers by infecting the computers with ZLoader malware and then using the C2 infrastructure to control victim computers

and to misappropriate confidential, sensitive, and high-value information. Dkt. 1 at ¶ 29-31; 96. Plaintiffs have suffered in excess of $5,000 dollars, and the Court credited this evidence in granting preliminary injunctive relief. *See* Dkt. 41. Accordingly, Plaintiffs has properly alleged a CFAA claim and is entitled to default judgment on this claim. Defendants conduct is precisely the type of activity the CF AA is designed to prevent. *See e. g.*, *Priority Payment Systems, LLC v. Jntrend Software Solutions*, 2016 WL 8809877, at *4-*5 (N.D. Ga. 2016) (defendant violated the CFAA after misappropriating the plaintiffs computer source code to build a competing system); *Sprint Nextel Corp.* v. *Ace Wholesale, Inc.*, 143 F.Supp.3d 1349 (N.D. Ga. 2015) (holding that defendants unlawful access of telecommunications company's protected computer systems and wireless network violated the CFAA); *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010) (defendant violated the CF AA when he accessed personal information in Social Security Administration databases for nonbusiness reasons); *Facebook, Inc. v. Fisher*, 2009 U.S. Dist. LEXIS 122578 (N.D. Cal. 2009) (CFAA violation where defendants allegedly engaged in a phishing and spamming scheme that compromised the accounts of Facebook users); *Physicians Interactive v. Lathian Sys., Inc.*, 2003 U.S. Dist. LEXIS 22868, *25 (E.D. Va. 2003) (CFAA violation where the defendant hacked into a computer and stole confidential information); *Microsoft Corp. v. Doe*,

2015 U.S. Dist. LEXIS 109729 (E.D. Va. Aug. 17, 2015) (O'Grady, J.) (CFAA violation for operating botnet); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 46951 (E.D. Va. Apr. 2, 2014) (Brinkema, J.) (same).

ECPA Claim. The ECPA prohibits "intentionally access[ing] without authorization a facility through which electronic communications are provided" or doing so in excess of authorization, and, in so doing, obtaining, altering, or preventing authorized access to an electronic communication while it is in electronic storage. 18 U.S.C. § 270l(a). Persons injured by violations of the ECPA may bring a civil suit to obtain injunctive relief and damages. *See e.g.*, *DIRECTV, Inc. v. Benson*, 333 F. Supp. 2d 440, 449 (M.D.N.C. 2004). The Complaint alleges that Plaintiffs servers and its licensed operating system at end user computers are facilities through which electronic communication services are provided. Dkt. 1 at ¶ 128. Defendants' conduct in propagating ZLoader violates the ECPA because Defendants break into computing devices and computer networks with the direct intention of acquiring the contents of sensitive communications be they e-mails, voice mails, or other communications types. *Id.* Defendants use software, installed without authorization on compromised computers to do so. *Id.* Obtaining stored electronic information in this way, without authorization, is a violation of the Electronic Communications Privacy Act. *See Global Policy Partners, LLC*, 686 F.

Supp. 2d 631, 635-637 (E.D. Va. 2009) (unauthorized access to e-mails was actionable under ECPA); *State Analysis, Inc. v. American Fin. Srvcs. Assoc.*, 621 F. Supp. 2d 309, 317-318 (E.D. Va. 2009) (access of data on a computer without authorization actionable under ECPA). Hacking into a computer and intercepting Internet communications clearly violates the ECPA. *See, e.g.*, *Sharma v. Howard County*, 2013 U.S. Dist. LEXIS 18890, 19 (D. Md. Feb. 12, 2013).

Accordingly, Plaintiff properly alleged an ECPA claim and default judgment on this claim is warranted.

Lanham Act Claims. Section 1114(1) of the Lanham Act prohibits use of a reproduction, counterfeit, copy or "colorable imitation" of a registered mark in connection with the distribution of goods and services where such use is likely to cause confusion or mistake or to deceive. *See* 15 U.S.C. *§* 1114(l)(a)). Here, the Complaint alleges that Defendants use Plaintiffs' registered, famous and distinctive trademarks in Internet domains designed to deceive victims into clicking on the links in e-mails and to blend in with normal network traffic, when those domains are being used to unlawfully send commands to victim computers or exfiltrate sensitive stolen data. Dkt. 1 at ¶¶ 72, 73, 96, 98, and 99. In this way, Defendants deceive victims, cause them confusion, and cause them to mistakenly associate Plaintiffs with this activity. *Id.* at 99, 99. Defendants' conduct also constitutes false designation of

origin under section 1125(a), causing confusion and mistakes as to Plaintiffs' affiliation with Defendants' malicious conduct. *See, e.g.*, *Brookfield Commc'ns, Inc. v. West Coast Entertainment Corp.*, 174 F. 3d 1036, 1066-67 (9th Cir. 1999) (entering_preliminary injunction under Lanham Act §l 125(a) for infringement of trademark in software and website code). The Complaint alleges this Lanham Act violation in detail as well. Dkt. 1 at ¶¶ 141-151. Thus, Plaintiff properly alleged these Lanham Act claims and default judgment is warranted.

Georgia's Computer Systems Protection Act Claims. Plaintiffs sufficiently alleges their causes of actions for computer trespass (OCGA § 16-9-93(6)) and computer invasion of privacy (OCGA § 16-9-93(c)) of Georgia's Computer Systems Protection Act (GCSPA). A person commits computer trespass when he "uses a computer or computer network with knowledge that such use is without authority and with the intention of" deleting any computer program or data; obstructing or interfering with use of a computer program or data; or altering, damaging, or causing to malfunction a computer, computer network, or computer program. OCGA § 16-9-93(a)(l)-(3). A person commits computer invasion of privacy when he uses a computer or computer network "with the intention of examining any employment, medical, salary, credit, or any other financial or

personal data relating to any other person with knowledge that such examination is without authority." OCGA § 16-9-93(c).

Plaintiffs sufficiently alleges Defendants' violations of computer trespass and computer invasion of privacy under the GCSPA. Defendants accessed Plaintiffs' customers' computers and Plaintiffs computers and computer networks without their knowledge (or authority), and with the intention to further the botnet, facilitate the ZLoader malware, and to steal, delete or remove data - either temporarily or permanently - from those computer and networks. Dkt. 1 at ¶ 56, 153, 177. As a result, Plaintiffs have been damaged by Defendants' conduct. Because Plaintiffs have properly pled these claims, default judgment should be entered against Defendants for violation of the GCSPA.

RICO Claim. "To state a claim for a violation of the federal RICO statute, a plaintiff has the burden of showing that (1) that the defendant (2) through the commission of two or more acts (3) constituting a 'pattern' (4) of 'racketeering activity' (5) directly or indirectly invests in, or maintains an interest in, or participates in (6) an 'enterprise' (7) the activities of which affect interstate or foreign commerce." *See McCulloch v. PNC Bank, Inc.*, 298 F.3d 1217, 1225 (11th Cir.2002) (citing 18 U. S.C. §§ 1962(a)-(c)). Under the Georgia RICO act, it is "unlawful for any person, through a pattern of racketeering activity or proceeds

derived therefrom, to acquire or maintain, directly or indirectly, any interest in or control of any enterprise, real property, or personal property of any nature, including money." *See* O.C.G.A. § 16-1 4-4(a). A "pattern of racketeering activity" means "at least two acts of racketeering activity in furtherance of one or more incidents, schemes, or transactions" that are interrelated. *Id.* § l 6-l 4-3(8)(A). A "racketeering activity" is the commission, attempt, solicitation of another, or coercing of another to commit a "crime which is chargeable by indictment" under one of forty categories of offenses. *Id. §* 16-14-3(9)(A)(i)-(xl).

To have standing to bring a civil claim under Georgia's RICO Act, a plaintiff must not only show a pattern of racketeering activity, but also "a direct nexus between at least one of the predicate acts listed under the RICO Act and the injury [the plaintiff] purportedly sustained." *Schoenbaum Ltd. Co. v. Lenox Pines, LLC*, 262 Ga.App. 457 (Ga. Ct. App. 2003) (internal quotation marks omitted). "To establish this nexus, the plaintiff must show that one of the predicate acts directly harmed it, not a third party." *Id.*

Here, taking the well-pleaded allegations of the Complaint as true, Plaintiffs have established that the ZLoader malware and related C2 infrastructure amounts to a violation of the federal and Georgia RICO Acts. Defendants developed and operated the ZLoader botnets worldwide by means of wire communication to

execute their fraudulent scheme. Dkt. 1 at ¶ 203. The ZLoader malware and related C2 infrastructure affected interstate and foreign commerce. *Id.* at ¶¶ 121, 122, 203, 205. And as a result of Defendant's pattern of racketeering activity, Plaintiffs' and their customers were directly injured by Defendants' conduct. *Id.* at ¶ 200. Accordingly, Plaintiffs properly alleged a violation of RICO and default judgment is warranted.

Conversion and Trespass to Chattel Claims. Under Georgia law, to make a prima facie case for the tort of conversion, "the plaintiff must show title to the property, possession by the defendant, demand for possession, and refusal to surrender the property, or an actual conversion prior to the filing of the suit." *Atlantic Coast Line R. Co. v. McRee*, 12 Ga.App. 137 (1913). Any distinct act of dominion and control wrongfully asserted over another's personal property, in denial of his right or inconsistent with his right, is a conversion of such property. *Lovinger v. Hix Green Buick Co.*, 110 Ga.App. 698, 699(1) (1964). The related tort of trespass to chattels applies where there is "[a]ny unlawful abuse of or damage done to the personal property of another." O.G.C.A. *§* 51-10-3; *see AT&T Mobility LLC v. Does 1-4*, 201 l WL 13213864, at *2 (N.D. Ga. 2011).

Here, the Complaint establishes that Defendants exercised dominion and authority over Plaintiffs proprietary Windows software, including Microsoft Excel

and Word, by injecting code that fundamentally changed important functions of the software, converted Plaintiffs' property, and were unjustly enriched with ill-gotten benefits reaped from the ZLoader malware and its victims. Dkt. 1 at ¶¶ 169-170.

Plaintiffs there have adequately alleged facts which are sufficient to state a claim for conversion and trespass to chattels.

Unjust Enrichment Claim. Under Georgia law, "[t]he theory of unjust enrichment applies when there is no legal contract and when there has been a benefit conferred which would result in an unjust enrichment unless compensated." *Smith Serv. Oil Co.* v. *Parker*, 250 Ga.App. 270 (Ga.Ct.App.2001). Thus, the essential elements of the claim are that (I) a benefit has been conferred, (2) compensation has not been given for receipt of the benefit, and (3) the failure to so compensate would be unjust. *Clarkv. Aaron's, Inc.*, 9 14 F.Supp.2d 1301, 1309 (N.D. Ga. 2012). Here, Plaintiffs state a claim for unjust enrichment. Defendants were unjust enriched at Plaintiffs' by promoting, distributing, and operating the ZLoader malware and related C2 infrastructure . Dkt. 1 at ¶¶ 169-170. Indeed, Defendants profited from the ZLoader malware and related C2 infrastructure. *Id.*at ¶ 170-172. Defendants' retention of the profits from the ZLoader malware and related C2 infrastructure would be inequitable and unjust. Plaintiffs are therefore entitled to default judgment under the unjust enrichment claim.

The well-pled allegations in Plaintiffs Complaint, which set forth the elements of each of Plaintiffs claims, are taken as true given Defendants' default. *See Pitts ex rel. Pitts v. Seneca Sports, Inc.*, 321 F.Supp.2d 1353, 1356, 1358 (11th Cir. 2004); *Tyco Fire & Sec., LLC v. Alcocer*, 218 Fed.App'x. 860, 863 (11th Cir. 2007); *see also* Fed. R. Civ. P. 8(b)(6). Accordingly, the only question is what remedy to afford Plaintiff.

D. A Permanent Injunction Should Issue to Prevent Further Irreparable Harm

A permanent injunction is appropriate where: (1) plaintiff has suffered an irreparable injury; (2) remedies available at law (e.g. monetary damages), are inadequate to compensate for that injury; (3) considering the balance of hardships between plaintiff and defendant, a remedy in equity is warranted; and (4) the public interest would not be disserved by a permanent injunction. *See eBay Inc. v. MercExchange, L.L.C.*, 547 U.S. 388 (2006).

1. Plaintiffs Have Suffered and are Likely to Suffer Irreparable Injury that Cannot Be Compensated Monetarily

Consumer confusion and injury to business goodwill constitute irreparable harm. *See, e.g.*, *PBM Prods., LLC v. Mead Johnson & Co.*, 639 F.3d 111, 127 (4th Cir. 2011) (false and misleading representations constituted irreparable harm, and warranted permanent injunction); *Int'l Labor Mgmt. C01p. 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") (citing *In Multi-Channel TV Cable Co. v. Charlottesville Quality Cable Operating Co.*, 22 F.3d 546 (4th Cir. 1994)); *MicroAire Surgical Instruments, LLC v. Arthrex, Inc.*, 726 F. Supp. 2d 604, 635 (W.D. Va. 2010) ("The loss of goodwill is a well-recognized basis for finding irreparable harm"). A finding of irreparable harm usually follows a finding of unlawful use of a trademark and a likelihood of confusion. *Ledo Pizza Sys. v. Singh*, 2013 U.S. Dist. LEXIS 146938, 9 (D. Md. Oct. 10, 2013); *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."). The Court previously found that the harm caused to Plaintiff by the ZLoader malware and related C2 infrastructure, in particular the confusing and misleading use of Plaintiffs' trademarks and brands, constitutes irreparable harm. Dkt. 41. To the extent that Defendants are able to continue to use domains bearing Plaintiffs' trademarks and brands in furtherance of their activities such irreparable harm would certainly continue in the future.

This finding is consistent with several cases that have concluded that computer malware operations and associated use of Microsoft's trademarks cause

irreparable harm. *See, e.g.*, *Microsoft Corp. v. Peng Yong et al.*, Case No. 1: 12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.) (injunction to dismantle botnet command and control servers); *Microsoft v. Piatti, et al.*, Case No. 1: 11-cv-101 7 (E.D. Va. 2011) (Cacheris, J.) (injunction to dismantle botnet command and control servers); *Microsoft Corporation v. John Does 1-27*, Case No. l:10-cv-156 (E.D. Va.) (Brinkema, J.) (same); *Microsoft v. John Does 1-11*, Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.) (same); *Microsoft Corp. et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.) (same); *FTC v. Pricewert LLC et al.*, Case No. 09-2407 (N.D. Cal. 2009) (Whyte J.) (injunction disconnecting service to botnet hosting company).

In addition to the irreparable harm caused to Plaintiffs goodwill, even the monetary harm caused by Defendants is and will be irremediable absent an injunction because Defendants are elusive cybercriminals whom Plaintiff is unlikely to be able to enforce a judgment against. *See, e.g.*, *Khepera-Bey v. Santander Consum. USA, Inc.*, 2013 U.S. Dist. LEXIS 87641, 13-14 (D. Md. June 21, 2013) ("circumstances[] such as insolvency or unsatisfiability of a money judgment, can show irreparable harm."); *accord Burns v. Dennis-Lambert Invs., Ltd. P'ship*, 2012 Bankr. LEXIS 1107, 9 (Bankr. M.D.N.C. Mar. 15, 2012) ("a preliminary injunction may be appropriate where 'damages may be unobtainable from the defendant

because he may become insolvent before final judgment can be entered.'"); *Rudolph v. Beacon Indep. Living LLC*, 2012 U.S. Dist. LEXIS 7075, 5 (W.D.N.C. Jan. 23, 2012) ("Irreparable harm exists here because of Defendant Beacon's continued occupancy of the Facility without paying any rents, particularly in light of the threat of insolvency by one or more Defendants .").

2. The Balance of Hardships Overwhelming Favors An Injunction

Because Defendants are engaged in an illegal scheme to defraud computer users and injure Plaintiff, the balance of equities clearly tips in favor granting an injunction. *See, e.g.*, *PBM Prods., LLC v. Mead Johnson & Co.*, 639 F.3d 11 1, 127 (4th Cir. 2011) (where defendant had no legitimate interest in "perpetuating the false and misleading" representations, balance of equities warranted injunction); *US Airways, Inc. v. US Airline Pilots Ass'n*, 81 3 F. Supp. 2d 710, 736 (W.D .N.C. 2011) (injunction appropriate where, in balance of the equities, denying injunction would result in "enormous disruption and harm" to plaintiff and the public, granting injunction would only require defendant to comply with existing legal duties); *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). On one side of the scales of equity rests the harm to Plaintiff and its customers caused by the Defendants' ongoing ZLoader operation, including ongoing

deceptive use of Plaintiffs' trademarks and brands in the C2 domains used in connection with the ZLoader malware. By contrast, on the other side rests no legally cognizable harm to Defendants because an injunction would only require them to cease illegal activities. For this reason, an ongoing permanent injunction is appropriate. *See US Airways*, 13 F. Supp. 2d at 736.

3. An Injunction is in the Public Interest

The public interest is clearly served by enforcing statutes designed to protect the public. *See, e.g.*, *PBM Prods., LLC v. Mead Johnson & Co.*, 639 F.3d 111, 127 (4th Cir. 2011) (preventing false or misleading representations constitutes a "strong public interest" supporting permanent injunction); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, 32 (E.D. Va. Jan. 6, 2014) (public interest weighed in favor of injunction to enforce CFAA); *BSN Med., Inc. v. Art Witkowski*, 2008 U.S. Dist. LEXIS 95338, 10 (W.D.N.C. Nov. 21, 2008) ("In a trademark case, the public interest is 'most often a synonym for the right of the public not to be deceived or confused.' . . . the infringer's use damages the public interest.") (citation omitted); *Dish Network LLC v. Parsons*, 2012 U.S. Dist. LEXIS 75386, 8-9 (W.D.N.C. May 30, 2012) (public interest weighed in favor of injunction to enforce ECPA).

Here, Plaintiff requests an injunction that will transfer permanent control of the existing C2 domains used in connection with the ZLoader malware to

Microsoft. As a result of such injunction, Plaintiffs will be able to protect itself and its customers from the threat of Defendants operations and can continue to assist victims in cleaning infected computers. Absent the requested injunction, the Defendants' existing infrastructure would be released back into Defendants' control, Defendants would be able to establish new malicious domains and associated infrastructure with impunity, and Defendants would be able to use that infrastructure to deceive computer users, issue instructions to infected computers, take control over them, and exfiltrate high value, sensitive and confidential information.

Given the risks the public will face absent an injunction, the calculus is clear. There is no risk that the injunction will impact any legitimate interest of any party. Neither Defendants nor any other party has come forward to assert any undue impact by Plaintiffs' control of the existing C2 domains used in connection with the ZLoader malware. In particular, the third-party domain registries responsible for administering the Defendants' C2 domains must simply carry out routine actions that they would take in the ordinary course of their business, namely transferring the domains to the permanent control of Plaintiffs. Directing such routine actions and reasonable cooperation to vindicate the public's interest, and ensure that the permanent injunction is not rendered fruitless, is authorized by the All Writs Act (28 U.S.C. § 1651(a) and the Court's equitable authority), will not offend Due Process,

does not interfere with normal operations, does not deprive any third party of any property interest and requires Plaintiffs to compensate the third parties for the assistance rendered.[1] Indeed, Plaintiff has conferred with relevant domain registries and they have no objection to the requested relief.

V. CONCLUSION

For the reasons set forth in this brief, and based on the Complaint, the evidence submitted in this case and the Court's prior orders, Plaintiff respectfully requests that the Court grant Plaintiffs' Motion for Default Judgment and Permanent Injunction.

[1] The All Writs Act provides that a court may issue all writs necessary or appropriate for the administration of justice. 28 U.S.C. § 165l(a); *see United States v. New York Tel. Co.,* 434 U.S. at 174 (authorizing order to third-party telephone company to assist in implementation of a pen register warrant); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, 30 (E.D. Va. Jan. 6, 2014) (authorizing relief similar to that requested herein); *United States v. X*, 601 F. Supp. 1039, 1042 (D. Md. 1984) (order to a third patty to provide "nonburdensome technical assistance"); *Moore v. Tangipahoa Parish Sch. Bd.,* 507 Fed. App'x. 389, 396 (5th Cir. 2013) (unpublished) ("The All Writs Act provides 'power to a federal court to issue such commands ... as may be necessary or appropriate to effectuate and prevent the frustration of orders it has previously issued in its exercise of jurisdiction otherwise obtained.'") (citing *New York Tel. Co.*, 434 U.S. at 172); *In re Application of United States for an Order Authorizing An In-Progress Trace of Wire Commc'ns Over Tel. Facilities*, 616 F.2d 1122, 1129 (9th Cir. 1980) (same); *In re Baldwin-United Corp.*, 770 F.2d 328, 338-339 (2d Cir. 1985) ("An important feature of the All-Writs Act is its grant of authority to enjoin and bind non-parties to an action when needed to preserve the court's ability to reach or enforce its decision in a case over which it has proper jurisdiction").

Dated: November 17, 2022 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

Gabriel M. Ramsey (*pro hac vice*)
Anna Z. Saber (*pro hac vice*)
CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111
Tel: (415) 986-2800
Fax: (415) 986-2827
gramsey@crowell.com
asaber@crowell.com

Emily Alban (*pro hac vice*)
Garylene Javier (*pro hac vice*)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Tel: (202) 624-2500
Fax: (202) 628-5116
ealban@crowell.com
gjavier@crowell.com

Richard Domingues Boscovich

(*pro hac vice*)
MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052-6399
Tel: (425) 704-0867
Fax: (425) 936-7329
rbosco@microsoft.com

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: November 17, 2022 Respectfully submitted,

/s/ Joshua D. Curry
Joshua D. Curry