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

MICROSOFT CORPORATION	)	
Plaintiff,	)	**CASE NO.**
	)	1: 17-CV-4566
v.	)	
	)	**<u>FILED UNDER SEAL</u>**
JOHN DOES 1-51, CONTROLLING MULTIPLE COMPUTER BOTNETS THEREBY INJURING MICROSOFT AND ITS CUSTOMERS	)	
Defendants.	)	

BRIEF IN SUPPORT OF MICROSOFT'S APPLICATION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE: PRELIMINARY INJUNCTION

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

MICROSOFT CORPORATION **Plaintiff,** **v.** **JOHN DOES 1-51, CONTROLLING MULTIPLE COMPUTER BOTNETS THEREBY INJURING MICROSOFT AND ITS CUSTOMERS** **Defendants.**	**CASE NO.** 1:17-CV-4566 **<u>FILED UNDER SEAL</u>**

BRIEF IN SUPPORT OF MICROSOFT'S APPLICATION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE: PRELIMINARY INJUNCTION

INTRODUCTION

Microsoft first detected the Gamarue malware in 2011 and subsequently identified it as one of the top malware threats plaguing consumers of Microsoft's Windows operating system. Further investigation by Microsoft and other anti-virus researchers revealed that Gamarue attempts to infect as many as three to four million computers each month. The infected computers known as a "bots" form a collective group of computers known as a "botnet," which is operated by Defendants using command and control ("C2") servers. The Defendants primarily use the Gamarue malware to surreptitiously infect victim computers with at least 80 additional types of malware, and using these C2 servers, the Defendants are able to deliver instructions to and control these infected "bots" in order to carry out malicious acts that harm Microsoft, its customers, and the public.

The Gamarue malware allows Defendants to spread every known variety of malware: ransomware to infect and lock a victims' computers until a ransom is paid; malware used to launch denial of service attacks using other infected "bot" devices, flooding the targeted networks and Internet sites with web traffic in order to disable these targets; and password stealers that collect victims' banking credentials for use and resale in underground markets on the Darkweb. Microsoft seeks this Temporary Restraining Order ("TRO") to stop the harm caused by Defendants' malware attacks of Microsoft Windows operating systems on victim computers. Microsoft requests an order that will allow it to block communications between Defendants and the infected computers, which will effectively disable the malware and also assist in the identification of victims currently operating the malware.

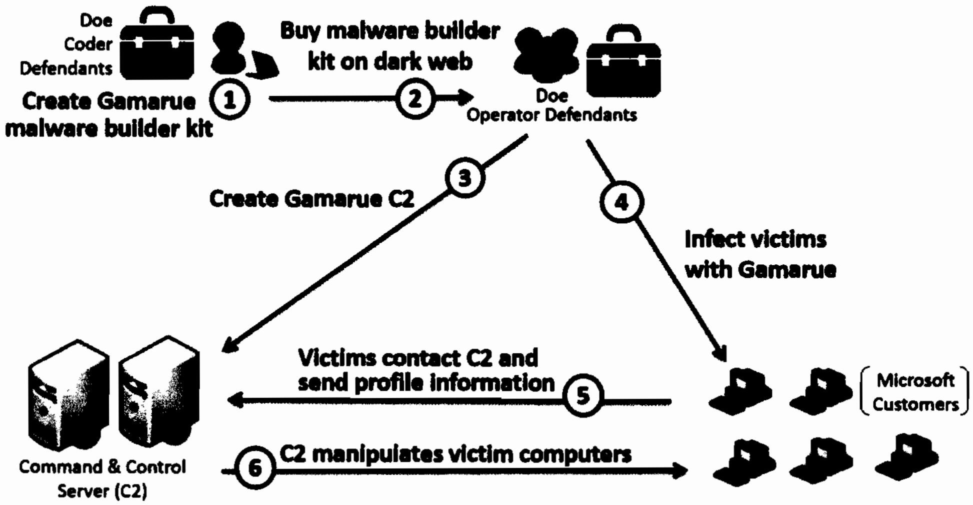
An *ex parte* application for a TRO is warranted and necessary here. First, given Defendants' abusive conduct, Microsoft is likely to succeed on the merits of its claims. Second, Defendants have caused Microsoft irreparable harm, including the ongoing loss of goodwill and brand integrity associated with the Microsoft Windows operating system that the Defendants secretly modify through malware infection. And Microsoft is not the only one harmed—with Gamarue, Defendants' carry out criminal and tortious activity, such as stealing sensitive information and mounting denial of service attacks, causing further untold harm on Microsoft's customers.

Third, the balance of hardships weighs in Microsoft's favor. Defendants' criminal activities serve no legitimate purpose, and Microsoft only seeks to block illegitimate communication between Defendants and infected computers. Thus, there is no hardship on Defendants or any third party. Fourth, the public interest is served by granting the TRO, because Defendants' actions inflict harm on millions of innocent, unsuspecting computer users and institutions around the world.

Additionally, *ex parte* relief is required here. Advanced notice will permit Defendants, who operate in a virtual world, to destroy evidence and disappear without a trace, thus rendering Microsoft's extensive investigation fruitless.

STATEMENT OF FACTS

Between three and four million computers encounter the Gamarue malware each month.[1] The below figure shows how the Defendants use Gamarue to operate a collection of unknowingly infected victim computers as a botnet through C2 servers.[2]


Doe Coder Defendants
Create Gamarue malware builder kit
1
Buy malware builder kit on dark web
2
Doe Operator Defendants
Create Gamarue C2
3
4
Infect victims with Gamarue
Victims contact C2 and send profile information
5
Microsoft Customers
C2 manipulates victim computers
6
Command & Control Server (C2)

In step 1, the "Coder Defendants" (Doe Defendants 1–5) develop the Gamarue malware and offer it for sale in a malware builder kit.[3] In step 2, the "Operator Defendants" (Doe Defendants 6-51) acquire the builder kit from the

[1] Declaration of Vishant Patel In Support Of Microsoft's Application For An Emergency *Ex Parte* Temporary Restraining Order And Order To Show Cause Re: Preliminary Injunction ("Patel Decl.") ¶¶ 5-7.

[2] Declaration of Rodelio G. Fiñones In Support Of Microsoft's Application For An Emergency *Ex Parte* Temporary Restraining Order And Order To Show cause Re: Preliminary Injunction ("Fiñones Decl.") ¶¶ 9-15; Declaration of Jean-Ian Boutin In Support Of Microsoft's Application For An Emergency *Ex Parte* Temporary Restraining Order And Order To Show cause Re: Preliminary Injunction ("Boutin Decl.") ¶¶ 6-10; Patel Decl. ¶¶ 8, 10.

[3] Fiñones Decl. ¶¶ 13-15.

Coder Defendants and use it to create and operate a botnet, as shown in steps 3–6.[4] In step 3, the Operator Defendants set up the "command and control" tier—comprised of C2 servers—to operate the infected "bots" that belong to their botnet.[5] There are at least 464 distinct botnets currently operated using Gamarue malware.[6]

The C2 servers reside at locations on the Internet called domains. Each resource on the web, such as a website like cnn.com, can be accessed through a unique domain.[7] This domain is often presented as a user friendly name like "cnn.com," while it actually corresponds to a unique alpha-numeric value IP address, such as 157.166.226.26.[8] The C2 servers for the Gamarue malware have resided at 1,214 domains that the Operator Defendants use to address and exchange information with the C2 servers,[9] and six such domains, listed in **Appendix A** to the Complaint, are currently in use.[10]

Each Gamarue C2 server domain, like any other domain, is managed by a

[4] *Id.*

[5] *Id.*

[6] Patel Decl. ¶ 5; Fiñones ¶ 14.

[7] Patel Decl. ¶ 11-12; Boutin ¶¶ 16, 29-32.

[8] *Id.*

[9] Patel Decl. ¶ 12; Fiñones ¶ 14.

[10] Patel Decl. ¶ 15.

registry service, which facilitates association of the domain with an IP address. The six Gamarue domains at issue in the present proceedings are managed by the registry services also listed in **Appendix A** to the Complaint.[11]

In step 4, the Operator Defendants infect the Microsoft Windows operating system on victim computers with the Gamarue malware to create the infection tier of the botnets.[12] These infections occur without authorization from Microsoft, the owner of Windows, or the victim computer owners, which license Windows from Microsoft. The Gamarue malware is spread via multiple vectors, including spam campaigns, exploit kits (i.e., delivery via other malware), downloaders, USB/portable drives, and social media services.[13]

As shown in step, 5, when Gamarue infects a new computer, it instructs the device to contact a C2 server over the Internet.[14] As depicted in step 6, this enables the Operator Defendants to send malicious instructions and additional malware to the infected victim computers without owner authorization.[15]

As part of step 6, the Operator Defendants (i) disable built-in Windows

[11] *Id.*

[12] Fiñones Decl. ¶¶ 9-15; Patel Decl. ¶¶ 8, 10; Boutin Decl. ¶¶ 6-10.

[13] Boutin Decl. ¶¶ 10-18, 21-28; Fiñones ¶ 14, 18-19, 21, 25-26; Patel Decl. ¶¶ 7, 10.

[14] Fiñones Decl. ¶¶ 9-15; Patel Decl. ¶¶ 8, 10; Boutin Decl. ¶¶ 6-10.

[15] *Id.*

security features, leaving victim computers vulnerable to further harm, (ii) alter the functionality of victims' computers and the Microsoft-licensed software installed on those computers, and (iii) download at least 80 different strains of malware to facilitate even greater harm.[16] The Gamarue malware and the additional malware that it loads, allow the Operator Defendants to (a) steal user account credentials or other personal and sensitive information for use and resale, (b) spy on users of infected computers to capture keystrokes, mouse actions and desktop activity, (c) capture any data (e.g., credentials) submitted by users of infected computers online through Microsoft's Internet Explorer and other browsers, (d) exercise control over infected computers, and (e) carry out additional criminal activity (e.g., fraud, identity and financial theft, ransom, spam, and attacks on other computers).[17]

Malware infections tarnish the reputation of Microsoft and its products, because consumers incorrectly attribute the harm caused by Gamarue to Microsoft's products.[18] This creates a serious risk that customers may abandon Microsoft's products, and once this occurs, there are significant challenges to winning the customers back.[19]

[16] Boutin Decl. ¶¶ 14, 20-23; 25.
[17] Fiñones Decl. ¶¶ 9-15; Patel Decl. ¶¶ 8, 10; Boutin Decl. ¶¶ 6-10.
[18] Fiñones Decl. ¶¶ 5-8, 20-23, 27-35; Patel Decl. ¶¶ 5-7.
[19] Fiñones Decl. ¶¶ 27-35.

RELIEF REQUESTED

Microsoft seeks to have the Court issue a TRO and subsequent preliminary injunction that requires the registry services listed in **Appendix A** to the Complaint to route the six Gamarue domains to Microsoft. As a result, victim computer communications intended for the Gamarue C2 servers will be directed to Microsoft—severing ties between the Gamarue C2 servers and the victim computers.[20] Microsoft can then take steps that enable infected computer owners to remove the Gamarue malware.[21]

LEGAL ARGUMENT

A TRO or preliminary injunction is warranted where the movant establishes: "(1) a substantial likelihood of success on the merits; (2) that it will suffer irreparable injury unless the injunction is issued; (3) that the threatened injury outweighs the harm the temporary restraining order would inflict on the non-movant; and (4) that the temporary restraining order would not be adverse to the public interest."[22] Microsoft has met these requirements here. Under similar circumstances caused by

[20] Patel Decl. ¶¶ 15-25, 35.

[21] *Id.*

[22] *Holmes v. Dominique*, No. 1:13-CV-04270-HLM, 2014 U.S. Dist. LEXIS 189469, at *2–3 (N.D. Ga. May 5, 2014) (*citing LSSI Data Corp. v. Comcast Phone, LLC*, 696 F.3d 1114, 1119 (11th Cir. 2012)).

different malware, Microsoft obtained TROs in fifteen prior cases involving cybercriminals who were committing malicious acts related to malware and botnets.[23]

I. Microsoft is Likely to Succeed on the Merits on Each of its Claims

The numerous claims set forth in the Complaint include: (1) Computer Fraud and Abuse Act ("CFAA") (18 U.S.C. § 1030), (2) Georgia Computer Systems Protection Act (O.C.G.A. § 16-9-93), (3) Lanham Act (15 U.S.C. §§ 1114 et seq.), (4) Uniform Deceptive Trade Practices Act (O.C.G.A. § 10-1-372), (5) Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962), (6) conversion and trespass (O.C.G.A. § 51-10-1 et seq.), and (7) the common law of tortious interference with contractual or business relations and (8) unjust enrichment. Microsoft is likely to succeed on all of these claims. Exemplary demonstrations of this success appear below.

A. <u>The Computer Fraud and Abuse Act</u>

Congress enacted the CFAA specifically to address computer crime.[24] "[A]ny computer with Internet access [is] subject [to] the statute's protection."[25]

[23] *See* Declaration of Michael Zweiback In Support Of Microsoft's Application For An Emergency *Ex Parte* Temporary Restraining Order And Order To Show Cause Re: Preliminary Injunction ("Zweiback Decl.") ¶¶ 3-7, Exs. 11-36.

[24] *See, e.g., Big Rock Sports, LLC v. AcuSport Corp.*, 2011 U.S. Dist. LEXIS 110995, 3 (E.D.N.C. Sept. 26, 2011).

[25] *Id.*

Inter alia, 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).

A "protected computer" is a computer "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communications in the United States."[26] 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."[27] In order to prosecute a civil claim under the CFAA, a plaintiff must demonstrate loss or damage in excess of $5,000.[28] The CFAA defines loss as "any reasonable cost to

[26] 18 U.S.C. § 1030(e)(2)(B).

[27] 18 U.S.C. § 1030(e)(6).

[28] *See* 18 U.S.C. § 1030.

any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[29] "Damage . . . means any impairment to the integrity or availability of data, a program, a system, or information."[30] The CFAA permits plaintiffs to aggregate multiple intrusions or violations for the purposes of meeting the $5,000 statutory threshold.

In sum, in order to prevail on their CFAA claim, Microsoft must establish that Defendants (1) accessed a protected computer; (2) without authorization; (3) for the purpose of obtaining information or defrauding others; and (4) resulting in loss or damage in excess of $5,000. Here, Defendants' conduct satisfies each of these elements.

First, each of the computers and computer networks infected or compromised by Defendants, in each case running Microsoft software licensed to the victims is, by definition, a protected computer.[31] Defendants target computers that connect to the Internet or other interfaces because the Gamarue malware requires the ability to

[29] 18 U.S.C. § 1030(e)(8).
[30] 18 U.S.C. § 1030(e)(11).
[31] 18 U.S.C. § 1030(e)(2)(B) (defining "protected computer" as a computer "used in interstate or foreign commerce or communication").

deliver instructions from C2 servers to infected devices over the Internet. Second, each server and computer compromised or infected by Defendants has been accessed without authorization—Defendants surreptitiously install the Gamarue malware on the infected machines without their owner's knowledge or consent.[32] Third, Defendants' illegal acts are carried out for the purpose of obtaining the highly sensitive information from victims via the infected computers and compromised networks.[33] Defendants, moreover, damage the integrity of computers and computer networks running Microsoft's operating systems and other Microsoft software—*inter alia*—by impairing the integrity of the Windows registry and file system.[34] Finally, the amount of harm caused by Defendants exceeds $5,000.[35]

Defendants' conduct is precisely the type of activity that the CFAA is designed to prevent.[36] Courts have observed that the CFAA was targeted at

[32] *See* Boutin Decl. ¶¶ 3, 12; Fiñones Decl. ¶¶ 28, 31-32; Patel Dec. ¶ 5.

[33] *See* Boutin Decl. ¶¶ 4, 12, 26, 32-33; Fiñones Decl. ¶¶ 10, 19, 23, 27.

[34] *See* Fiñones Decl. ¶ 20.

[35] *See* Fiñones Decl. ¶ 33-34; Boutin Decl. ¶ 34.

[36] *See, e.g., Facebook, Inc. v. Fisher*, No. C09-05842JF, 2009 WL 5095269, at *2-3 (N.D. Cal. Dec. 21, 2009) (granting a TRO under CFAA where defendants allegedly engaged in a phishing and spamming scheme that compromised the accounts of Facebook users); *Physicians Interactive v. Lathian Sys.*, No. CA-03-1193-A, 2003 U.S. Dist. LEXIS 22868, at *30-31 (E.D. Va. Dec. 5, 2003) (granting TRO and preliminary injunction under CFAA where defendant hacked into a computer and stole confidential information); *Global Policy Partners, LLC*

"computer hackers (e.g., electronic trespassers)."[37]

B. The Georgia Computer Systems Protection Act

This Act addresses the problem of "computer related crime"[38] including computer theft, computer trespass, and computer invasion of privacy.[39]

Computer Theft: A person commits "computer theft" if he "uses a computer or computer network with knowledge that such use is without authority and with the intention of: (1) Taking or appropriating any property of another . . . [or] (2) Obtaining property by any deceitful means or artful practice."[40] The term "property" includes "computers, computer networks, computer programs, data, financial instruments, and services."[41]

Defendants know their use of Microsoft's operating system and its customers' computers is without authority. The Gamarue malware takes control of infected computers and uses them for illicit purposes without the victims' knowledge or

v. Yessin, 686 F. Supp. 2d 631, 635-37 (E.D. Va. 2009) (accessing computer using credentials that did not belong to defendant actionable under the CFAA).

[37] *State Analysis, Inc. v. Am. Fin. Srvcs. Assoc.*, 621 F. Supp. 2d 309, 315 (E.D. Va. 2009) (citation omitted).

[38] O.C.G.A. § 16-9-91.

[39] *Id.* at § 16-9-93; *SCQuARE Int'l, Ltd. v. BBDO Atlanta, Inc.*, 455 F. Supp. 2d 1347, 1368 (N.D. Ga. 2006).

[40] O.C.G.A. § 16-9-93(a)(1)–(2).

[41] O.C.G.A. § 16-9-92(13).

permission.[42] Defendants surreptitiously take data from infected computers, including keystrokes, mouse actions, and credentials submitted online.[43]

Computer Trespass: A person commits "computer trespass" if he "uses a computer or computer network with knowledge that such use is without authority and with the intention of: (1) Deleting or in any way removing . . . any computer program or data from a computer . . . (2) Obstructing, interrupting or in any way interfering with the use of a computer program or data; or (3) Altering, damaging, or in any way causing the malfunction of a computer, computer network, or computer program."[44]

Defendants' use of infected Microsoft operating systems and victim computers is without authority.[45] Defendants use the Gamarue malware with the intention of installing plugins and/or additional malware, as well as stealing data from infected computers.[46] Defendants utilize Gamarue to alter the functionality of Microsoft products on victims' computers, thus interfering with victims' use of those

[42] *See* Boutin Decl. ¶¶ 3, 12; Fiñones Decl. ¶¶ 28, 31-32; Patel Dec. ¶ 5.
[43] Fiñones Decl. ¶¶ 9-15; Patel Decl. ¶¶ 8, 10; Boutin Decl. ¶¶ 6-10.
[44] O.C.G.A. § 16-9-93(b)(1)–(3).
[45] *See* Boutin Decl. ¶¶ 3, 12; Fiñones Decl. ¶¶ 28, 31-32; Patel Dec. ¶ 5.
[46] Fiñones Decl. ¶¶ 9-15; Patel Decl. ¶¶ 8, 10; Boutin Decl. ¶¶ 6-10.

products.[47]

Computer Invasion of Privacy: A person commits computer invasion of privacy if he "uses a computer . . . with the intention of examining . . . financial or personal data relating to any other person with knowledge that such examination is without authority."[48] Defendants use the Gamarue malware to access data on infected computers running Microsoft products, including monitoring keystrokes and mouse actions, and data submitted by the computer owners online (e.g., credentials).[49] As explained, Defendants know such examination is without authority.

C. The Lanham Act

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. Defendants infect Microsoft's and its customers' computers with the Gamarue malware, and by doing so, change the functionality of the

[47] Fiñones Decl. ¶¶ 9-15, 28, 31-32; Patel Decl. ¶¶ 5, 8, 10; Boutin Decl. ¶¶ 3, 6-10, 12.

[48] O.C.G.A. § 16-9-93(c).

[49] Fiñones Decl. ¶¶ 9-15; Patel Decl. ¶¶ 8, 10; Boutin Decl. ¶¶ 6-10.

Windows operating systems and other software on the infected computers.[50] The adulterated versions of Microsoft products carry out malicious activities and have degraded performance, but the products continue to bear Microsoft's registered trademarks, such as the "Microsoft" and "Windows" marks.[51] Thus, Defendants use Microsoft's registered marks in commerce in connection with the adulterated versions of Microsoft products. This is likely to confuse victims into mistakenly associating Microsoft and its products with the fraudulent activity of Defendants. This is a clear violation of the Lanham Act and Microsoft is likely to succeed on the merits.

In addition to constituting infringement under section 1114 of the Lanham Act, Defendants' conduct also constitutes false designation of origin under section 1125(a), which prohibits use of a registered mark that:

> is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person.[52]

As mentioned, Defendants use Microsoft's registered marks in connection with the

[50] *See id.*
[51] *See* Fiñones Decl. ¶¶ 29-35.
[52] 15 U.S.C. § 1125(a)(1)(A).

adulterated versions of Microsoft products created on victim computers—including Microsoft® and Windows®.[53] This use is likely to cause confusion among consumers, who are likely to mistakenly associate Microsoft with Defendants' fraudulent activity and products.[54]

Similarly, Defendants' conduct is also likely to cause dilution by tarnishment of Microsoft's marks. Section 1125(c) provides that "the owner of a famous mark that is distinctive . . . shall be entitled to an injunction against another person who . . . commences use of a mark or trade name in commerce that is likely to cause . . . dilution by tarnishment of the famous mark." Microsoft owns the "Microsoft," "Internet Explorer" and "Windows" marks, which are widely recognized as a designation of the source of Microsoft's goods and services.[55] Defendants use these famous marks in commerce in conjunction with Defendants' adulterated versions of Microsoft products.[56]

This activity is therefore a clear violation of Lanham Act § 1125(a) and (c) and Microsoft will likely succeed on the merits.[57]

[53] *Id.*

[54] *Id.*; *see also* Boutin Decl. ¶ 34.

[55] *See* Fiñones Decl. ¶¶ 29-35.

[56] *See id.* ¶¶ 20, 29-35.

[57] *See Garden & Gun, LLC v. Twodalgals, LLC*, 2008 U.S. Dist. LEXIS 79982 (W.D.N.C. 2008) (granting preliminary injunction against misleading use of

D. Uniform Deceptive Trade Practices Act

Defendants' acts violate the Uniform Deceptive Trade Practices Act, which penalizes a party that:

- Passes off goods or services as those of another (§ 10-1-372(a)(1));
- Causes likelihood of confusion or of misunderstanding as to the source, sponsorship, approval, or certification of goods or services (§ 10-1-372(a)(2));
- Causes likelihood of confusion or of misunderstanding as to affiliation, connection, or association with or certification by another (§ 10-1-372(a)(3));
- Represents that goods are original or new if they are altered (§ 10-1-372(a)(6));
- Represents that goods or services are of a particular standard, quality, or grade or that goods are of a particular style or model, if they are of another (§ 10-1-372(a)(7)); or
- Engages in any other conduct which similarly creates a likelihood of confusion or of misunderstanding (§ 10-1-372(a)(12)).[58]

trademarks under Section 1125(a)); *IHOP Corp. v. Langley*, 2008 U.S. Dist. LEXIS 112056 at *1-3 (same; granting TRO); *Am. Online v. IMS*, 24 F. Supp. 2d 548, 551-52 (E.D. Va. 1998) (misuse of trademark in e-mail headers violated §1125(a), and also constituted trademark "dilution" under §1125(c)); *Brookfield Commc'ns.*, 174 F. 3d 1036, 1066-67 (entering preliminary injunction under Lanham Act §1125(a) for infringement of trademark in software and website code); *Hotmail Corp. v. Van$ Money Pie, Inc.*, 1998 U.S. Dist. LEXIS 10729, *12-13 (N.D. Cal. 1998) (granting preliminary injunction; copying the Hotmail trademarks in "e-mail return addresses" constituted false designation of origin; also constituted trademark "dilution" under §1125(c)).

[58] O.C.G.A. §§ 10-1-372.

Defendants violate the Act by using the Microsoft registered marks in connection with the adulterated versions of Microsoft's Windows operating system and other software, such as Microsoft® and Windows®.[59] Specifically, Defendants pass off the adulterated versions of Microsoft products as products of Microsoft.

Defendants cause a likelihood of confusion or misunderstanding as to the source of the adulterated Microsoft products and as to the affiliation, connection, or association with or certification by Microsoft.[60] Defendants represent that the adulterated Microsoft products are original Microsoft products and are thus of a particular standard, despite the fact that these products have been altered in a way that degrades their performance; and Defendants engage in conduct that creates a likelihood of confusion regarding Microsoft's association with Defendants' fraudulent conduct.

E. **Conversion and Trespass**

Defendants' acts constitute trespass and conversion in violation of Georgia law. Many other courts have held that these torts are applicable to the context of electronic records and/or computer hacking.[61]

[59] Fiñones ¶¶ 20, 29-35.

[60] *See* Fiñones Decl. ¶¶ 20, 29-35.

[61] *E.g.*, *Microsoft Corp. v. Doe*, No. 1:13cv139, 2014 U.S. Dist. LEXIS 48398, at * 24–25 (E.D. Va. Jan. 6, 2014) ("The unauthorized intrusion into an individual's

Trespass: Georgia law defines trespass as "[a]ny unlawful abuse of or damage done to the personal property of another."[62] Defendants commit trespass by damaging Microsoft's proprietary software, including the Windows operating system, as well as the computers of Microsoft and its customers by infecting these computers with the Gamarue malware. The damage inflicted includes detrimental changes to the functionality of the Windows operating system and other software on the infected computers.[63] Defendants willfully cause this damage by infecting computers with the Gamarue malware through a number of vectors.[64] Defendants use the infected computers to commit crimes, such as identity theft and denial of service attacks to disable sites on the Internet.[65]

Conversion: Georgia law provides that "[t]he owner of personalty is entitled to its possession" and "[a]ny deprivation of such possession is a tort for which an action lies."[66] Although not stated in the statute, some Georgia courts require plaintiffs to prove the following elements when the defendant has unlawfully come

computer system through hacking, malware, or even unwanted communications supports actions under [claims for trespass to chattels and conversion].").

[62] O.C.G.A. § 51-10-3.

[63] *See* Fiñones Decl. ¶¶ 20, 29-35; Boutin Decl. ¶¶ 34-35.

[64] Boutin Decl. ¶¶ 13-15; Fiñones Decl. ¶¶ 12-15; Patel Decl. ¶¶ 5-9.

[65] Fiñones Decl. ¶¶ 9-15; Patel Decl. ¶¶ 8, 10; Boutin Decl. ¶¶ 6-10.

[66] O.C.G.A. § 51-10-1.

into possession of the relevant property: (1) proof of ownership or title to the disputed property, or the right to immediate possession of the property; (2) actual possession of the property by the defendant; and (3) the value of the property.[67]

Here, Microsoft owns the Microsoft software and products, including the Windows operating system, running on the infected computers, which it licenses to the computer users.[68] Defendants have taken possession of Microsoft's property by targeting Microsoft's proprietary products with the Gamarue malware, altering the functionality of the Microsoft products installed on victim computers, and using the adulterated Microsoft products to control the infected computers.[69] This infection changes Microsoft's products and deprives Microsoft of its right to control the content, functionality, and nature of its software. Microsoft's proprietary products generate significant annual revenue and are thus valuable.[70]

[67] *Carter v. Butts Cnty.*, 821 F.3d 1310, 1324 (11th Cir. 2016). Additional elements (e.g., plaintiff demanded return of the property and defendant's refusal to do so) apply if defendant lawfully came into possession of the property, *see Williams v. Nat'l Auto Sales, Inc.*, 287 Ga. App. 283, 285 (Ct. App. 2007), which is not the case here.

[68] *See* Fiñones Decl. ¶¶ 20, 29-35; Boutin Decl. ¶¶ 34-35.

[69] Fiñones Decl. ¶¶ 9-15; Patel Decl. ¶¶ 8, 10; Boutin Decl. ¶¶ 6-10.

[70] Fiñones Decl. ¶ 30; *accord* Microsoft Corp., Annual Report (Form 10-K) (August 2, 2017).

F. **Tortious Interference with Contractual or Business Relations**

Microsoft is entitled to relief for Defendants' tortious interference with Microsoft's business relations. This is because (1) Defendants acted improperly and without privilege by infecting Microsoft's and its customers' computers with the Gamarue malware and infecting those computers with Gamarue malware; (2) Defendants acted purposefully and with malice with the intent to injure Microsoft and its customers; (3) Defendants' actions have altered and degraded Microsoft's products and causing Microsoft's customers to discontinue using its products and services; and (4) as a result of Defendants' unauthorized and intentional conduct, Microsoft has suffered financial injury.[71] These actions by Defendants were "malicious" as there was no "[]authorized interference, or any interference [with] legal justification or excuse."[72] The sole purpose of the Gamarue malware is to infect victim computers to obtain highly sensitive information, among other things.[73] There is therefore clear evidence of Microsoft's claim for tortious interference with its business relations.

[71] *See Labat v. Bank of Coweta*, 218 Ga. App. 187, 189 (1995) (elements to recover a claim for tortious inference with business relations).

[72] *Id.*; *see also* Fiñones Decl. ¶¶ 9-15; Patel Decl. ¶¶ 8, 10; Boutin Decl. ¶¶ 6-10.

[73] Fiñones Decl. ¶¶ 9-15; Patel Decl. ¶¶ 8, 10; Boutin Decl. ¶¶ 6-10.

G. Unjust Enrichment

Unjust enrichment occurs when (1) the plaintiff has conferred a benefit on the defendant and (2) equity requires the defendant to compensate for that benefit.[74] Here, Defendants alter Microsoft products, including the Windows operating system, for financial gain.[75] Defendants exploit the widespread distribution and use of Microsoft's software and services in order to propagate the botnets operated using Gamarue malware, steal victims' information, and engage in other malicious activity.[76] The Coder Defendants profit by selling the Gamarue kit to the Operator Defendants, and the Operator Defendants profit by carrying out cyberattacks or stealing credentials for banking and credit card fraud.[77] It is inequitable for Defendants to retain these benefits; equity requires them to compensate Microsoft.

II. Irreparable Harm Will Result Unless a TRO and Preliminary Injunction are Granted

No monetary remedy could repair the harm to Microsoft and its customers if Defendants are permitted to continue operating and expanding these botnets. Other courts have concluded that the "immediate and irreparable harm" caused by similar

[74] *Schütz Container Sys., Inc. v. Mauser Corp.*, No. 1:09-CV-3609-RWS, 2012 U.S. Dist. LEXIS 44012, 110–11 (N.D. Ga. Mar. 28, 2012).
[75] Fiñones Decl. ¶¶ 9-15; Patel Decl. ¶¶ 8, 10; Boutin Decl. ¶¶ 6-10.
[76] Fiñones Decl. ¶¶ 29-35; Patel Decl. ¶¶ 5-9.
[77] Fiñones Decl. ¶¶ 9-15; Patel Decl. ¶¶ 8, 10; Boutin Decl. ¶¶ 6-10.

malware and botnets warranted an *ex parte* TRO and preliminary injunction.[78] These courts acknowledged the substantial irreparable harm that botnets cause to Microsoft, its customers, and Internet users generally.[79] Here, Microsoft and the public face the same irreparable harm from the Gamarue malware that was found to exist in previous cases.[80] Thus, entry of an *ex parte* TRO and an Order to Show Cause why a preliminary injunction should not issue are warranted.

If the requested relief is not granted, the Gamarue malware will continue to spread and infect the computers of Microsoft and its customers.[81] This injury is irreparable because customers generally lack the technical knowledge, skills, and ability to remedy the stealth infection by Gamarue.[82] In the absence of the requested relief, Microsoft and its customers will remain under constant threat of the unauthorized intrusion into and abuse of their computers that is associated with Gamarue.[83] Long term injury of this type constitutes irreparable harm warranting the entry of the requested relief.[84] This harm includes spying, identity theft, and

[78] *See* Zweiback Decl. ¶¶ 3-7, Exs. 11-36.
[79] *See id.*
[80] *See id.*
[81] Fiñones ¶¶ 25-26.
[82] Boutin Decl. ¶¶ 33-34.
[83] *See* Fiñones Decl. ¶¶ 9-15; Patel Decl. ¶¶ 8, 10; Boutin Decl. ¶¶ 6-10.
[84] *See Arminius Schleifmittel GmbH v. Design Indus., Inc.*, No. 1:06CV00644, 2007 WL 534573, at *6 (M.D.N.C. Feb. 15, 2007) (finding irreparable harm

invasion of privacy.

Microsoft will suffer irreparable harm to its brand and reputation unless Defendants' conduct is enjoined. Microsoft has invested substantial resources in developing high-quality products and services, including the Windows operating system and other software. Due to the high quality of Microsoft's products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, established a strong brand, and developed the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade.[85] Microsoft has registered trademarks representing the quality of its products and services and its brand, including the Windows marks.[86]

Defendants' activities injure Microsoft and its reputation, brand, and goodwill. Customers affected by the Gamarue malware may incorrectly believe that Microsoft or Windows is the source of their computer problems.[87]

because defendant's action "will have significant and continuous long-term effects").

[85] Fiñones Decl. ¶¶ 29-35.

[86] *Id.*

[87] *See id.*

Additionally, Microsoft devotes significant computing and human resources to combating Gamarue malware infections, helping customers determine whether or not their computers are infected, and if so, cleaning them.[88] Customers' frustration from malware infections diminishes their regard for Windows and Microsoft, and tarnishes Microsoft's reputation and goodwill. There is also a serious risk that customers may leave Microsoft's products in favor of other platforms because of Defendants' activities.[89] After customers make this switch, there is a high risk that these customers will not return to Microsoft products due to the cost of switching to new products and the harm caused by Defendants prior to the switch.[90] This type of brand-related injury and customer harm is irreparable and is one of many reasons that the relief requested in this motion should be granted.[91]

[88] *Id.*; Boutin ¶¶ 33-34.

[89] *See, e.g.*, Fiñones Decl. ¶ 33.

[90] Fiñones Decl. ¶¶ 29-35.

[91] Other courts have found that this type of injury satisfies the "irreparable harm" requirement for granting a preliminary injunction. *See, e.g.*, *Adidas AG v. Footballbangkok.com*, No. 16-60220-CIV-COHN/SELTZER, 2016 U.S. Dist. LEXIS 23780, at *6 (S.D. Fla. Feb. 26, 2016) ("Defendants are selling goods bearing unauthorized, infringing copies of Plaintiffs' Marks . . . . [A]llowing Defendants to continue this illegal conduct would cause irreparable harm to Plaintiffs by damaging the reputation and goodwill associated with their genuine trademarked . . . goods.").

III. The Balance of Hardships Tip Sharply in Microsoft's Favor

Defendants will suffer no harm to any legitimate interest if an *ex parte* TRO and preliminary injunction are issued to re-route communications to the Gamarue C2 domains to Microsoft. The Gamarue domains serve no legitimate purpose and are used solely to support Gamarue.[92] An *ex parte* TRO also preserves the evidence of the botnets' structure and illegal activities, as well as evidence of the injury to victims.[93]

There will be only negligible impact on third-party domain registries that will implement part of the proposed order. The proposed order directs these third parties to take simple steps, in the course of their normal business operations, to redirect the Gamarue infrastructure and assist in preserving evidence.[94] This limited assistance is necessary to ensure effective implementation of the requested order and is authorized under the All-Writs Act, 28 U.S.C. § 1651.[95] Conversely, if a TRO and preliminary injunction do not issue, Gamarue malware will continue to inflict irreparable injury on Microsoft, its customers, and the public.

[92] *See* Patel Decl. ¶¶ 10-21.

[93] Patel Decl. ¶¶ 22-25.

[94] *See id.*

[95] *United States v. New York Tel. Co.*, 434 U.S. 159, 173–74 (1977) (upholding district court's order to non-party telephone company under All-Writs Act to provide assistance to FBI needed to carry out court order).

IV. The Public Interest Will Be Served by the Issuance of a TRO and Preliminary Injunction

A TRO and preliminary injunction will protect not only the interest of Microsoft and its customers, but also the interest of the general public. Every consumer, company, governmental agency, or other entity with access to the Internet is at risk of irreparable injury by the botnets operated using the Gamarue malware. In a case where the defendant hacked into plaintiff's computer and stole confidential information, the court granted the TRO noting the existence of "a strong public interest in granting preliminary injunctive relief" and noted that "[t]his Court has an obligation to enjoin any alleged computer hackers from continuing to attack and steal [plaintiff's] proprietary information."[96] Similarly here, there is an overwhelming public interest in halting the operation of this malware while Microsoft proceeds with its claims.[97]

V. *Ex Parte* Relief is Necessary to Stop the Irreparable Harm to Microsoft and the Public

Rule 65 of the Federal Rules of Civil Procedure and Civil Local Rule 7-5(B) permit an *ex parte* TRO where the moving party sets forth facts that show an immediate and irreparable injury and why notice should not be required.[98] Here,

[96] *Physicians Interactive*, 2003 U.S. Dist. LEXIS 22868, at *30–31.
[97] *See* Boutin Decl. ¶¶ 33-34; Fiñones Decl. ¶¶ 29-35.
[98] Fed. R. Civ. P. 65(b)(1); L.R. 7.5(B).

without the requested TRO, the injury to Microsoft, its customers and the public will continue unabated, irreparably harming Microsoft's reputation, brand and goodwill. In order for the TRO to be effective at all, it must issue *ex parte*. The extraordinary factual circumstances here warrant such relief.

If notice is given prior to the issuance of a TRO, Defendants will move the botnets operated using the Gamarue malware to different C2 servers, at different domains and IP addresses.[99] They will restart their criminal activities under different online aliases, continue to carry out the malicious activities discussed above, and destroy information relating to the issues in this case—rendering Microsoft's efforts to investigate and combat their abuse moot.[100]

It is well-established that *ex parte* relief is appropriate where, as here, notice would render the requested relief fruitless. District courts in the Eleventh Circuit have issued *ex parte* TROs where notice would enable the non-moving party to take evasive action that would thwart the moving party's ability to obtain meaningful relief.[101] Here, the danger imposed by advanced notice is real and not vague or speculative. There is specific evidence that botnet operators have attempted to

[99] *See* Patel Decl. ¶¶ 22-25; Fiñones Decl. ¶¶ 34-35; Zweiback Decl. ¶¶ 4-5.

[100] *See id.*

[101] *See, e.g.*, *Adidas*, 2016 U.S. Dist. LEXIS 23780, at *3.

evade enforcement attempts where they had notice, such as by moving their C2 servers.[102] In February 2010, the Eastern District of Virginia found good cause to issue an *ex parte* TRO and supplemental *ex parte* TRO suspending 276 Internet domains used to control a malicious botnet.[103]

Additionally, if notice is given in advance of a TRO, evidence of the Gamarue malware distribution may be destroyed. An Uninstall Gamarue command enables Defendants to uninstall Gamarue from infected machines, thereby destroying evidence of Defendants' conduct.[104] Under such circumstances, courts have issued *ex parte* TROs.[105]

VI. Microsoft Will Make Extraordinary Efforts to Provide Notice and to Serve the Complaint

Immediately upon entry of the requested *ex parte* TRO, Microsoft will undertake extraordinary efforts to effect formal and informal notice of the preliminary injunction hearing to Defendants and to serve the complaint. Microsoft will provide notice of the preliminary injunction hearing and a copy of the summons,

[102] Zweiback Decl. ¶¶ 4-5.
[103] *See id.* ¶¶ 3-7; Exs. 11-36.
[104] Fiñones Decl. ¶ 18; Boutin Decl. ¶ 18.
[105] *See AT&T Broadband v. Tech Commc'ns, Inc.*, 381 F.3d 1309, 1319–20 (11th Cir. 2004) (affirming *ex parte* search and seizure order based on evidence that in the past defendants and persons similarly situated hid evidence once notice was given).

complaint, TRO motion and supporting documents to the Defendants by publication and any other method ordered by this Court.

VII. Conclusion

For the reasons stated above, Microsoft respectfully requests that this Honorable Court grant its motion for a TRO and order to show cause regarding a preliminary injunction. Microsoft further respectfully requests that the Court permit notice of the preliminary injunction hearing and service of the Complaint by alternative means.

[*Signature on next page*]

Dated: November 14, 2017

Respectfully submitted,

Donald M. Houser (GA No. 157238)
Andrew J. Tuck (GA No. 402306)
ALSTON & BIRD LLP
1201 West Peachtree Street
Atlanta, GA 30309
Tel.: (404) 881-7000
Fax: (404) 881-7777
donald.houser@alston.com
andy.tuck@alston.com

Michael Zweiback (*pro hac vice* application pending)
Erin Coleman (*pro hac vice* application pending)
ALSTON & BIRD LLP
333 S. Hope Street, 16th Floor
Los Angeles, CA 90071
Tel.: (213) 576-1000
Fax: (213) 576-1100
michael.zweiback@alston.com
erin.coleman@alston.com

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

Attorneys for Plaintiff Microsoft Corp.

CERTIFICATION OF COMPLIANCE

Pursuant to L.R. 7.1(D), N.D. Ga., counsel for Plaintiff hereby certifies that this Brief 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 14, 2017

Respectfully submitted,

Donald M. Houser (GA No. 157238)
Andrew J. Tuck (GA No. 402306)
ALSTON & BIRD LLP
1201 West Peachtree Street
Atlanta, GA 30309
Tel.: (404) 881-7000
Fax: (404) 881-7777
donald.houser@alston.com
andy.tuck@alston.com

Michael Zweiback (*pro hac vice* application pending)
Erin Coleman (*pro hac vice* application pending)
ALSTON & BIRD LLP
333 S. Hope Street, 16th Floor
Los Angeles, CA 90071
Tel.: (213) 576-1000
Fax: (213) 576-1100
michael.zweiback@alston.com
erin.coleman@alston.com

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

Attorneys for Plaintiff Microsoft Corp.