Randall D. Haimovici (*Pro Hac Vice Approved*)
rhaimovici@shb.com
Rachael M. Smith (*Pro Hac Vice Approved*)
rxsmith@shb.com
SHOOK, HARDY & BACON L.L.P.
One Montgomery, Suite 2700
San Francisco, California 94104-4505
Telephone: 415.544.1900
Facsimile: 415.391.0281

Tony M. Diab (Nevada State Bar No. 12954)
tdiab@shb.com
SHOOK, HARDY & BACON L.L.P.
5 Park Plaza, Suite 1600
Irvine, California 92614-2546
Telephone: 949.475.1500
Facsimile: 949.475.0016

Robert J.B. Flummerfelt (Nevada State Bar No. 11122)
rflummerfelt@hotmail.com
Rami Hernandez (Nevada State Bar No. 13146)
rhernandeznsj@hotmail.com
CANON LAW SERVICES, LLC
7251 W. Lake Mead Blvd., Suite 300
Las Vegas, Nevada 89128
Telephone: 702.562.4144
Facsimile: 702.866.9868

Attorneys for Plaintiff
MICROSOFT CORPORATION

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

MICROSOFT CORPORATION, Plaintiff, vs. NASER AL MUTAIRI, an individual; MOHAMED BENABDELLAH, an individual; VITALWERKS INTERNET SOLUTIONS, LLC, d/b/a NO-IP.com; and DOES 1-500, Defendants.	)	Case No. 2:14-cv-00987-GMN-GWF **MICROSOFT'S MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF ITS MOTION FOR DEFAULT JUDGMENT** **(Hearing Requested)** <u>Filed Concurrently Herewith</u>: Motion for Default Judgment; Declaration of Jason Lyons; Declaration of Rachael M. Smith; [Proposed] Order

INTRODUCTION

Plaintiff Microsoft Corporation ("Microsoft") respectfully submits this Motion for Default Judgment against Defendant Naser Al Mutairi and Defendant Mohamed Benabdellah ("Defendants"). This lawsuit derives from the intentional and malicious harm to Microsoft customers as a result of malware developed by Defendants. Defendants developed and spread malware specifically and purposefully designed to abuse users of Microsoft's software. In particular, Defendants developed malware designed to mimic and or infiltrate Microsoft's software so as to allow unlawful access to Microsoft's customers' personal computers. Defendants did so by developing malware that illegally circumvents security measures Microsoft develops and employs to protect against unlawful access. Defendants' wrongful conduct entitles Microsoft to statutory damages, as well as injunctive relief to enjoin the development of other malware.

FACTUAL BACKGROUND

Microsoft is the provider of the Windows operating system and other software and services. (Comp. ¶ 55.) Microsoft has invested substantial resources in developing high-quality products and services for its customers. (*Id.*) Due to the high quality and effectiveness 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, has established a strong brand, and has developed the Microsoft name and the names of its products and services into strong and famous world-wide symbols. (*Id.*)

One of the ways in which Microsoft continues to provide high-quality products and services is to combat the distribution of malware infecting its consumers' computers running the Windows operating system. To do this, Microsoft monitors data it receives from its anti-virus and anti-malware software running on Windows computers. (Comp. ¶ 27.) When the anti-virus software detects and cleans the malware from the computer, it sends data back to Microsoft and from this data, Microsoft can determine which malware was removed and whether the malware was instructing the infected computer to reach out and communicate with other computers. (*Id.*)

In early 2014, Microsoft began investigating the top malware threats impacting Windows computers and uncovered that cybercriminals were using sub-domains owned and leased by

Vitalwerks Internet Solutions, LLC ("Vitalwerks") to facilitate the spread of over 245 different types of malware. (Comp. ¶¶ 27-28.) Further investigation revealed that the majority of criminal actors using Vitalwerks' services for illicit purposes were related to two similar malware families, Bladabindi and Jenxcus. (*Id.* at Fig. 2, ¶ 37.) As of July 2014, Microsoft had detected over 7,486,833 instances of Windows computers that had encountered one or more versions of Bladabindi or Jenxcus malware in the past year. (*Id.* ¶ 41.)

Defendant Mutairi created the Bladabindi and Jenxcus malware, a malware that is closely related in function to Bladabindi. (Compl. at ¶ 38.) Defendant Benabdellah created a popular variant of the Jenxcus malware. (*Id.* at ¶ 39.) Defendant Mutairi makes the Bladabindi and Jenxcus malware available for others to use and download on the Internet. (*Id.* at ¶ 38.) He also publishes updates to the malware online and provides instructions and tutorials to others on how to use and customize the malware. (*Id.*)

Bladabindi/Jenxcus can be downloaded by other cybercriminals who then can use the malware's dashboard to customize the malware to suit their needs. (Compl. ¶ 40.) The dashboard is a user interface that allows the cybercriminal to control and execute commands on the infected computer. (*Id.*) The dashboard can display a list of all infected computers' IP addresses and locations, and it can even display real time screen shots of the infected computers' desktops. (*Id.*; *see also id.* at Fig. 4.) Cybercriminals can execute a variety of commands through the dashboard including viewing the victim's computer screen in real time, turning on the victim's computer camera to watch or record the victim, recording keystrokes, stealing passwords stored on the victim's computer, remotely terminating security features on the victim's computer, and remotely executing files, such as additional malware, on the computer. (*Id.* at ¶¶ 42-43, 52-53, Fig. 8.)

Defendants have created and distributed Bladabindi/Jenxcus malware that permits other hackers to gain control over and use the infected computers for criminal purposes. With this malware, third-party criminals can control a large group of computers, or a botnet, to execute a variety of cybercrimes such as distributing spam, denial of service attacks on other computers or networks, theft of financial and banking data, eavesdropping, stalking, or spying. (Compl. ¶ 44.)

Infected computers part of a botnet are a valuable commodity on the black market and can be sold, leased, or swapped by one criminal group to another. (*Id.*)

Bladabindi/Jenxcus software has been designed to be downloaded and assume control over individuals' computers without Microsoft's or the users' knowledge or consent. (Compl. ¶ 58.) Computer users unknowingly will download the malware by using a colleague or friend's infected thumb-drive, accessing an Internet link or website where the malware downloaded is staged, or download other programs containing instructions to download the malware. (*Id.* ¶ 45.) The malware has also been designed to mislead computer users into clicking on and running the malware by disguising itself as a legitimate or familiar file. (*Id.* at ¶¶ 46, 59.) Once the malware is activated, it will instruct the user's computer to communicate with the cybercriminal's computer and let it know that it is ready to receive instructions or commands. (*Id.* at ¶¶ 48-49.) This occurs without the users' knowledge unless or until the malware is detected by an anti-malware program. (*Id.* at ¶ 60.)

Defendants, by creating and distributing malware, have caused Microsoft and its consumers substantial harm. With the malware, bad actors can steal users' banking credentials, such as online user names, passwords, and account numbers. (Compl. ¶ 61.) When a user conducts transactions online, the hacker can monitor the user's keystrokes and capture home and work addresses, telephone numbers, credit card information and social security numbers. (*Id.*) The hacker can also execute a variety of commands invading the user's privacy including watching the user or the user's computer screen in real time. (*Id.*) Defendants have also cause Microsoft harm because the malware infects computers with the Windows operating system, a product owned by Microsoft that it licenses to its customers. (*Id.* at ¶ 58.) Additionally, Microsoft has had to devote significant computing and human resources to combating the distribution of Bladabindi/Jenxcus malware and helping its customers with their infected computers. (*Id.* at ¶ 56.)

LEGAL STANDARD

I. The *Eitel* Factors Weigh In Favor Of A Default Judgment.

Requesting a default judgment against a party is a two-step process under Rule 55 of the Federal Rules of Civil Procedure. *Gordon v. Me & You, Inc.*, 2014 WL 2770290, at *2 (D. Nev. Jun. 18, 2014). First, the clerk must enter default against a party "against whom a judgment for affirmative relief is sought [and] has failed to plead or otherwise defend, and that failure is shown by affidavit or otherwise." Fed. R. Civ. P. 55(a). Second, after the moving party has sought entry of default by the clerk, it may then seek a default judgment under 55(b).

The district court has the sole discretion to enter a default judgment under Rule 55. *Trustees of the Teamsters v. Beavers*, 2014 WL 298736, at *2 (D. Nev. Jan. 27, 2014). The Ninth Circuit has identified the following factors for a court to consider when determining whether to grant default judgment:

> (1) the possibility of prejudice to the plaintiff, (2) the merits of plaintiff's substantive claim, (3) the sufficiency of the complaint, (4) the sum of money at stake in the action; (5) the possibility of a dispute concerning material facts; (6) whether the default was due to excusable neglect, and (7) the strong policy underlying the Federal Rules of Civil Procedure favoring decisions on the merits.

Eitel v. McCool, 782 F.2d 1470, 1472 (9th Cir. 1986). "In applying this discretionary standard, default judgments are more often granted than denied." *PepsiCo v. Triunfo-Mex, Inc.*, 189 F.R.D. 431, 432 (C.D. Cal. 1999). Once the clerk has entered default, the factual allegations of the complaint, with the exception of those relating to the amount of damages, are taken as true. *Trustees of the Teamsters*, 2014 WL 298736, at *2; *see also Sprint Nextel Corp. v. Thuc Ngo*, 2014 WL 869406, at *1 ("By his default, Defendant is deemed to have admitted the well-pleaded averments of the complaint except as to the amount of damages."). The moving party must "prove all damages sought in the complaint," and "[i]f sufficiently documented and detailed, damages claims may be fixed by an accounting, declarations, or affidavits." *Trustees of the Teamsters*, 2014 WL 298736, at *2; *see also Sprint Nextel Corp.*, 2014 WL 869406, at *2 (noting that the court can rely on declarations in determining damages).

Here, the Court should grant a default judgment against Defendants. First, Microsoft has requested that the Clerk enter a default against the Defendants, and the default was entered. (ECF Dkt. Nos. 42-43.) Second, as discussed below, the *Eitel* factors weigh in favor of a default judgment.

//

//

A. The Possibility of Prejudice to Microsoft.

The first Eitel factor "considers whether Plaintiff will suffer prejudice if default is denied." *Warner Bros. Home Entertainment Inc. v. FilmAndMusicUSA, LLC*, 2013 WL 447 8956, at *3 (C.D. Cal. Aug. 20, 2013). Prejudice occurs when the plaintiff is "denied the opportunity to resolve its claim in court." *Id.*

Microsoft will be greatly prejudiced if it is not able to permanently enjoin Defendants from creating, promoting, and distributing the Bladabindi/Jenxcus malware or to seek compensation for the harm these Defendants have caused. Without a judgment, Microsoft will be without recourse to permanently stop the spread of the malware infecting Microsoft's and its customers' computers running the Windows software. Moreover, Microsoft's ability to refer these individuals for possible prosecution with U.S. or foreign authorities will be hampered if it is unable to seek a judgment in this case.

B. The Merits of Microsoft's Claims and Sufficiency of the Complaint.

The second and third *Eitel* factors look to whether the "complaint sufficiently states a claim for relief under the 'liberal pleading standards embodied in Rule 8' of the Federal Rules of Civil Procedure." *Gordon*, 2014 WL 2770290, at *2 (*citing Danning v. Lavine*, 572 F.3d 1386, 1389 (9th Cir. 1978)). Microsoft has sufficiently stated a claim against Defendants in the Complaint for violation of the Computer Fraud and Abuse Act and Nevada's Unlawful Acts Regarding Computers and Information Services Statute.[1]

1. Computer Fraud and Abuse Act.

Microsoft asserts that Defendants violated the Computer Fraud and Abuse Act ("CFAA") because they "knowingly cause[d] the transmission of a program, information, code, or command, and a result of such conduct, intentionally causes damage without authorization, to a protected computer." U.S.C. § 1030(a)(5)(A); *see also* Comp. ¶¶ 63. The "CFAA was designed to prevent the sort of unauthorized access and other fraudulent activity effectuated by malware and botnet activity." *Microsoft Corp. v. Does 1-18*, 2014 WL 1338677, at *6 (E.D. Va. Apr. 2, 2014); *see also State*

[1] Microsoft also asserted in the Complaint that Defendants violated the Anti-Cybersquatting Consumer Protection Act and were liable for common law trespass, conversion, and negligence. Microsoft is not seeking a default judgment as to these claims.

LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1130 (9th Cir. 2009) ("[The CFAA] was originally designed to target hackers who accessed computers to steal information or to disrupt or destroy computer functionality, as we as criminals who possessed the capacity to 'access and control high technology processes vital to our everyday lives.'" (citation omitted)).

Microsoft has stated a sufficient CFAA claim. First, Defendants have knowingly caused the transmission of Bladabindi/Jenxcus malware because they have created, distributed, and promoted the use of this malware to other criminal actors through the Internet and other means. *See Int'l Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006) (finding that "transmission" includes sending through the Internet). Next, Defendants' conduct was intentional and unauthorized. Defendants created a computer program the sole purpose of which is to infect unsuspecting users' computers with malware and execute commands that control and steal information from those computers. Defendants' conduct and the resulting infection and control over user computers was not authorized by Microsoft who owns the operating system running on the infected computers or by the computer users themselves.

Additionally, Defendants' conduct caused damage to protected computers. 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." 18 U.S.C. § 1030(e)(2)(B). Computers infected with Defendants' malware qualify as protected computers because they have Internet access. *See U.S. v. Nosal*, 676 F.3d 854, 959 (9th Cir. 2012) (finding that "all computers with Internet access" are protected computers); *Roadlink Workforce Solutions, L.L.C. v. Malpass*, 2013 WL 5274812, at *5 (W.D. Wash. 2013) (holding that defendant had pled sufficient facts that the computer at issue was a "protected computer" because it "was able to send and receive email communication and therefore would need to have internet access"); *Microsoft Corp. v. Does 1-18*, 2014 WL 1338677, at *6 (finding that end-users' computers infected with malware are "protected computers"); *see also* Comp. ¶¶ 40-45, 48-49 (alleging that the infected computers are controlled remotely through the Internet) and ¶ 27 (alleging that infected computers send data back to Microsoft if malware is detected).

Last, Microsoft has sufficiently pled that the protected computers have been damaged pursuant to 18 U.S.C. § 1030(e)(8). District courts in the Ninth Circuit have found that a computer is damaged when a hacker has infiltrated a computer, such as by stealing passwords, requiring the computer user to take corrected measures to prevent further hacking activities. *See Multiven, Inc. v. Cisco Systems, Inc.*, 725 F.Supp.2d 887, 894-95 (N.D. Cal. 2014) (discussing collection of cases in Washington and California).

2. Nevada's Unlawful Acts Regarding Computers and Information Services.

Microsoft also asserts that Defendants violated the Unlawful Acts Regarding Computers and Information Services Statute ("UARC"). The UARC prohibits a person from "knowingly, willfully and without authorization" modifying, damaging, destroying, disclosing, using, transferring, concealing, taking, retaining possession of, copying, obtaining or attempting to obtain access to, permitting access to or causing to be accessed, or entering "data, a program or any supporting documents which exist inside or outside a computer, system or network." N.R.S. § 205.4765(1). UARC also prohibits similar conduct in regards to "equipment or supplies that are used or intended to be used in a computer, system or network" or simply directing such activities at "a computer, system or network." N.R.S. § 205.4765(2)-(3). UARC also makes a person subject to liability for "knowingly, willfully and without authorization" obtaining and disclosing, publishing, transferring, or using "a device used to access a computer, network or data," or introducing, causing to be introduced or attempting to introduce a "computer contaminant into a computer, system or network." N.R.S. § 205.4765(4)-(5). A "computer contaminant" is broadly defined to include programs or data that has the ability to contaminate, corrupt, damage, destroy, disrupt, modify, record, or transmit data or other information contained in a computer, system, or program without the owner's consent. N.R.S. § 205.4737.

Here, Microsoft has pled that Defendants Mutairi and Benabdellah knowingly, willfully and without authorization published and transferred the Bladabindi/Jenxcus malware to the Doe Defendants, and the Does knowingly, willfully and without authorization used the malware to access victims' computers, including the Microsoft operating system and data on those computers in violation of sections 205.4765(4) and (5).

C. The Sum of Money at Stake.

As for the fourth *Eitel* factor, just like the harm caused by Defendants' malware, the sum of money at stake is not inconsequential. Every year Microsoft expends a substantial amount of resources to fix and protect against the harm caused by the Bladabindi/Jenxcus malware. Microsoft incurs costs for increased equipment, bandwith, and personnel to develop counter measures, investigate malware infections, remove malware from customers' computers, and address user complaints as a result of malware infections. With approximately seven million computers infected with Bladabindi/Jenxus alone at the time this lawsuit was filed, the potential costs of combating future and more sophisticated malware created by Defendants without any procedural abatement would be significantly greater than what was spent to combat the Bladabindi/Jenxus malware threat.

D. The Possibility of Disputed Material Facts and Whether Default was Due to Excusable Neglect.

There is little to no possibility that there are disputed material facts or whether default was due to excusable neglect of the Defendants. The factual allegations of Microsoft's complaint and the supporting evidence provided in the declarations and exhibits with Microsoft's motion for a temporary restraining order show that Defendants are responsible for the creation, distribution, and/or promotion of the Bladabindi/Jenxcus malware. Defendants were served with the Summons and Complaint, but they have chosen not to participate in this litigation or reach out to the Court in any way. Defendant Benabdellah deleted or removed several of his e-mail accounts after being served in this case, and Defendant Mutairi admitted that he is the defendant from Algeria and apologized for his actions. (Smith Decl. ¶¶ 2-5.) There is no evidence in this case that either Defendant's default is due to excusable neglect.

E. Policy Favoring Decisions on the Merits.

As for this last factor, Defendants' failure to appear, respond, or otherwise defend against Microsoft's complaint make a resolution on the merits impossible. Although resolution on the merits is preferable, when a defendant refuses to litigate a case, Rule 55 permits the court to enter a default judgment. The other *Eitel* factors favoring default judgment in this case outweigh the policy favoring a decision on the merits.

II. Microsoft Seeks Injunctive Relief and Compensatory Damages.

Pursuant to the CFAA, Microsoft is entitled to seek permanent injunctive relief and compensatory damages for "damage" and "loss" caused by the violations. *See* 18 U.S.C. § 1030(g). These include costs associated with investigating the intrusive activities and taking remedial measures to mitigate the harm. *See United Factory Furnishings Corp. v. Alterwitz*, 2012 WL 2138115, at *2 (D. Nev. Jun. 13, 2012) (finding that plaintiff had sufficiently pled damages under CFAA because it responded to the intrusion "by conducting a damages assessment [and] obtaining a mirror image of computer equipment"); *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.Supp.2d 1025, 1039 (N.D. Cal. 2012) ("Costs associated with investigating intrusions into a computer network and taking subsequent remedial measures are losses within the meaning of the statute."). Moreover, damages under the CFAA include loss of business and goodwill. *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 935 (9th Cir. 2004) ("When an individual or firm's money or property are impaired in value, or money or property is lost, or money must be spent to restore or maintain some aspect of a business affected by a violation, those are 'economic damages.'"). Microsoft may also seek damages "for any response costs, loss or injury" under UARC. *See* N.R.S. § 205.511(1)(a), (c). Response costs are defined as "any reasonable costs that arise in response to and as a proximate result of" a violation of the statute and include costs relating to investigation, ascertaining loss or damages, and mitigation or prevention of future loss or damages. *Id.* at § 205.4759(1)-(2).

First, Microsoft's request for a permanent injunction that prohibits Defendants from further distributing or promoting the use of the Bladabindi/Jenxcus malware is warranted. "The standard for a permanent injunction is essentially the same as for a preliminary injunction, with the exception that the plaintiff must show actually success, rather than a likelihood of success." *U.S. v. Wilson*, 2010 WL 1849338, at *2 (D. Nev. May 6, 2010). Microsoft has met its burden for a permanent injunction. This Court has already granted Microsoft's request for a preliminary injunction based on the pleadings, briefing, and supporting declarations and exhibits submitted in this action, finding that there was good cause to believe that Defendants engaged in acts and practices that violate the CFAA and UARC, that unless restrained, their actions will cause immediate and irreparable harm, and that

Microsoft is likely to prevail on its CFAA and UARC claims. (*See* ECF Dkt. No. 38, Order for Preliminary Junction at ¶¶ 4-6.) Additionally, if the Court grants a default judgment against Defendants, Microsoft meets the actual success requirement. Microsoft, therefore, requests that the Court permanently enjoin Defendants from engaging in the conduct prohibited in the preliminary injunction order.

Second, Microsoft requests that the Court award $ 750,000 in compensatory damages. These damages include the costs to investigate the malware infections and the loss to Microsoft's business and goodwill as a result of the infections. (Lyons Decl. ¶¶ 3-4.) These types of damages are recoverable under the CFAA and UARC.

CONCLUSION

Pursuant to Federal Rule of Civil Procedure Rule 55, Microsoft requests that the Court enter a default judgment against Defendants Mutairi and Benabdellah based on their failure to respond or otherwise defend this action. Microsoft additionally requests that the Court permanently enjoin Defendants from distributing or otherwise promoting the use of the Bladabindi/Jenxcus malware and award Microsoft $ 750,000 in damages.

Dated: October 29, 2014

SHOOK, HARDY & BACON L.L.P.

/s/ Randall D. Haimovici
RANDALL D. HAIMOVICI
RACHAEL M. SMITH

Attorneys for Plaintiff Microsoft Corporation