IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

MICROSOFT CORPORATION, a Washington corporation, and FS-ISAC, INC., a Delaware corporation, Plaintiffs, v. JOHN DOES 1-8, CONTROLLING A COMPUTER BOTNET THEREBY INJURING PLAINTIFFS, AND THEIR CUSTOMERS AND MEMBERS, Defendants.	Civil Action No: 1:14-cv-811 LOG/TCB

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

I. INTRODUCTION

Plaintiffs Microsoft Corporation and FS-ISAC, Inc. ("Plaintiffs") seek a default judgment and permanent injunction tailored to prevent Defendants John Does 1-8 from continuing to operate the malicious computer botnet known as the Shylock botnet. As set forth in Plaintiffs' pleadings and the Court's previous orders, the Shylock botnet is a network of computers infected with malicious software ("malware") that Defendants use to steal online banking information, passwords, and other personal information used to and carry out theft and financial fraud. Prior to issuance of this Court's Temporary Restraining Order and Preliminary Injunction in this action, Defendants controlled the Shylock botnet through IP addresses and internet domains used to relay instructions to infected computers. Plaintiffs now seek to bring this case to final conclusion by way of a permanent injunction that will prevent Defendants from retaking control of the Shylock botnet once this case is closed.

Plaintiffs request an injunction (1) prohibiting Defendants from operating or propagating the Shylock botnet; (2) permanently transferring ownership of malicious domains identified in the Court's preliminary injunction order to Microsoft. This injunctive relief is required to prevent further harm to Plaintiffs and the general public that would be caused if Defendants retake control of the Shylock infrastructure before additional infections abate. A permanent injunction is the only way to afford relief and abate future harm in this case, particularly given the that, in the absence of such relief, the command and control domains would revert to the Defendants who would be able to misuse and intrude upon Microsoft's Windows operating system and the computers of Microsoft's customers, continue to grow and control the botnet, stealing financial credentials, money, and personal data.

Plaintiffs duly served Defendants with the Complaint, Summons, and all pleadings in this action in a manner consistent with Due Process and this Court's instructions. Plaintiff's served Defendants by email and publication on July 8, 2014 at the website http://botnetlegalnotice.com/shylock/ and further served Defendants by email on July 14, 2014, January 8, 2015, and January 30, 2015. Defendants failed to respond. The record establishes the

elements of each of Plaintiffs' claims and also establishes the need for injunctive relief.

II. FACTUAL BACKGROUND

This action arises out of violations of federal and state law caused by Defendants' operation of the Shylock botnet. Defendants are the persons responsible for operating IP addresses and Internet domains used to propagate and control the Shylock botnet. A botnet is a collection of user computers infected with malware. Dkt. 21, Declaration of Vishant Patel, ¶ 4. This malware places the infected computers under the control of the individuals or an organization who operates the botnet. *Id.* Defendants communicate with infected computers over the Internet and use them to conduct their illegal acts. *Id.* ¶ 7. Shylock is a highly sophisticated botnet designed to intrude upon Microsoft's Windows operating system to steal money from financial accounts of owners of Shylock-infected computers. *Id.* Shylock inflicts extensive damage on infected computers. *Id.* ¶ 71-77. After infecting user computers with Shylock, Defendants can survey constantly the online banking activities of the unknowing victims. *Id.* Defendants' goals are to steal victims' financial account login IDs, passwords, and other personal identifying information in order to steal their money and their identities. *Id.*

Shylock botnets have a two-tiered architecture. Dkt. 21, ¶ 17-18. The lowest tier—referred to as the "Infection Tier"—consists of user computers infected with Shylock malware. *Id.* The second tier—referred to as the "Command and Control Tier"—consists of specialized computers that Defendants use to communicate with the infected user computers in the Infection Tier. *Id.* The Shylock Command and Control Tier includes IP addresses and Internet domains that the Shylock malware instructs infected computers to automatically reach out to once an internet connection is established. *Id.* Because the Shylock Command and Control infrastructure relies on IP addresses and domains, which are under the control of U.S. registrars and hosting companies, it is possible to disable the Shylock botnet by taking control of, and redirecting traffic to, U.S. based infrastructure.

On June 27, 2014, the Court entered a TRO that disabled the Shylock botnet's command and control infrastructure. Dkt. 16. The Court subsequently entered a Preliminary Injunction to

ensure that Defendants' malicious infrastructure cannot be used to cause further harm pending final resolution of this case. Dkt. 33.

When the Court issued the TRO and Preliminary Injunction, the Court found good cause to permit service of Plaintiffs' Complaint and related materials by alternative means pursuant to Rule 4(f)(3). Dkt. 16 at 7. The Court has directed that, under the circumstances, appropriate means of service sufficient to satisfy Due Process include emails to email accounts associated with Defendants and publication on a publically available Internet website. *Id.*

The Court further granted Plaintiffs the ability to pursue discovery in order to obtain further contact and identifying information regarding Defendants. Doe discovery is now complete. Dkt. 47. Because Defendants used fake contact information and stolen credit card numbers to set up these IP addresses and Internet domains comprising the Shylock botnet Command and Control Infrastructure, Defendants' true identities remain unknown. Dkt. 48-1, Declaration of Jacob M. Heath ("Heath Decl.") ¶¶ 4, 6.

Plaintiffs' Doe Discovery Efforts

Over the past six months, Plaintiffs have issued subpoenas to domain registrars, hosting companies, email providers, and other Internet service providers ("collectively ISPs") in an effort to obtain additional information regarding Defendants' identities. Heath Decl. ¶¶ 2, 3. Plaintiffs issued a first wave of subpoenas shortly after execution of the Court's Temporary Restraining Order. Heath Decl. ¶ 4. Based on information obtained during Plaintiffs' first wave of doe discovery, Plaintiffs sent subpoenas and informal discovery requests to additional ISPs. Heath Decl. ¶ 4. Plaintiffs also conducted telephone interviews with persons of interest. Heath Decl. ¶ 5.

Plaintiffs' doe discovery efforts yielded several names, addresses, and email addresses that were previously unknown to Plaintiffs, as well as various credit card account numbers used to pay for services associated with the Shylock botnet. Heath Decl. ¶ 4. Further investigation revealed that the names, addresses, and credit card information used by Defendants were fake or stolen. Heath Decl. ¶ 4.

Plaintiffs identified six individuals residing abroad who have been associated with infrastructure for the Shylock botnet over the past year. Heath Decl. ¶ 5. These individuals were determined to be hosting service resellers or the owners of services that were being leveraged or purchased, but from whom additional information about the specific identities of the Defendants was not available. A number of the resellers of services used by the Defendants are located beyond the Court's subpoena power in non-Hague Convention jurisdictions, and thus there is no reasonably available means to attempt to obtain further information from them about the Defendants. Plaintiffs have used all reasonably available formal and informal means to investigate the true identities of the Defendants. Heath Decl. ¶¶ 5, 6.

Plaintiffs have exhausted their ability to investigate Defendants' true identities using civil discovery tools, despite their best efforts and the exercise of reasonable diligence to determine Defendants' identities. Heath Decl. ¶ 6.

Service of Process on Defendants

The Court authorized service by email and publication on June 27, 2014. On July 8 and subsequently on July 14, 2014, Plaintiffs served email addresses associated with Defendants' IP addresses and Internet domains. Heath Decl. ¶ 7. Plaintiffs also served defendants by publication on July 8, 2014 at the website http://botnetlegalnotice.com/shylock/. Heath Decl. ¶ 8. Plaintiffs used an email tracking service to monitor whether service emails were received and read. Heath Decl. ¶ 7. A number of the known email addresses were in operation and successfully received the service of process emails at that time.

During the course of doe discovery, Plaintiffs identified 15 additional email addresses of interest associated with Shylock botnet infrastructure. Heath Decl. ¶ 9. These emails consist of recovery emails associated with previously identified email addresses and alternative email contact for domains and IP addresses associated with the Shylock botnet. Heath Decl. ¶ 9. On January 8, 2015, Plaintiffs served these additional email addresses and also re-served the functioning email addresses previously served during the first wave of service. Heath Decl. ¶ 11. Given that the email addresses were the point of contact actually used by the Defendants to

register the botnet domains and IP addresses (in conjunction with fake or stolen identity information such as names, addresses and credit card numbers), the email addresses are the only available point of contact with Defendants, and given the nature of their electronic activities, are the point of contact most likely to reach them. The complaint and notice were again served in early January 2015, in an abundance of caution, both to the email addresses to which notice had already successfully been sent, as well as to email addresses discovered during the discovery process.

The time for Defendants to answer or respond to the complaint expired 21 days after service of the summons—at the latest, on August 4, 2014 (21 days after email service). Heath Decl. ¶ 13. The Clerk entered Defendants' default pursuant to Federal Rule of Civil Procedure 55(a) on February 3, 2015.

The Court's Preliminary Injunctive Relief

The Court made several factual findings in the course of issuing preliminary injunctive relief to Plaintiffs. Among other findings, the Court concluded that:

- The Court has jurisdiction
- Defendants have used the IP addresses and domains identified by Plaintiffs to control a malicious computer botnet
- Unless enjoined, Defendants are likely to engage in conduct that violates the CFAA, ECPA, Lanham Act, and the common law doctrines of trespass to chattels, conversion, and unjust enrichment;
- Defendants' conduct causes irreparable harm

Dkt. 33 at 1-3. Based on these findings, the Court enjoined Defendants from further violations of law and ordered U.S. domain registries to cause domains registered by Defendants to resolve to Microsoft severs. The Court further ordered the transfer of non-registered domains to Plaintiffs and directed U.S. Internet service providers to block traffic to IP addresses and domains associated with the Shylock botnet.

The Court's order was extremely effective in disrupting the Shylock botnet. As discussed in previous briefs, at the center of Defendants' malicious infrastructure are the Shylock command and control servers—represented by three Internet domains Defendants use to host the Shylock malware, including the executable files used to infect user computers and the configuration files used to control user computers. Dkt. 6 at 7. By disabling the command and control servers, the Court's Temporary Injunction and Preliminary Restraining order crippled Defendants' command and control infrastructure.

III. LEGAL STANDARD

Rule 55 of the Federal Rules of Civil Procedure authorizes the entry of a default judgment when a defendant fails to plead or otherwise defend in accordance with the Federal Rules. *Tweedy v. RCAM Title Loans, LLC*, 611 F. Supp. 2d 603, 605 (W.D. Va. 2009) (citing *United States v. Moradi*, 673 F.2d 725, 727 (4th Cir. 1982)). The clerk of court's interlocutory "entry of default" pursuant to Federal Rule of Civil Procedure 55(a) provides notice to the defaulting party prior to the entry of default judgment by the court. In turn, Federal Rule of Civil Procedure 55(b)(2) "authorizes courts to enter a default judgment against a properly served defendant who fails to file a timely responsive pleading." *LPS Default Solutions, Inc. v. Friedman & MacFadyen, P.A.*, 2013 U.S. Dist. LEXIS 108486, at *2-3 (D. Md. Aug. 2, 2013). Default judgment is appropriate when the adversary process has been halted because of unresponsive party. *SEC v. Lawbaugh*, 359 F. Supp. 2d 418, 421 (D. Md. 2005). Upon default, the well-pled allegations in a complaint as to liability are taken as true. *Id.* Here, the Clerk has entered Defendants' default under Rule 55(a) (Dkt. 49), and Defendants have received notice of same.

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)).

Courts may order injunctive relief in conjunction with default judgments. *E.g., Trs. of the Nat'l Asbestos Workers Pension Fund v. Ideal Insulation, Inc*., 2011 U.S. Dist. LEXIS 124337, at *12 (D. Md. Oct. 27, 2011) (collecting cases).

IV. DISCUSSION

A. Due Process Has Been Satisfied

Plaintiffs have 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 email 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., FMAC Loan Receivables v. Dagra,* 228 F.R.D. 531, 534 (E.D. Va. 2005) (acknowledging that courts have readily used Rule 4(f)(3) to authorize international service through non-traditional means, including email); *Mullane v. Central Hanover Bank & Trust Co*., 339 U.S. 306, 314 (1950) (discussing Due Process requirements). Email service and Internet publication are particularly appropriate here given the nature of Defendants' conduct and use of email as the primary means of communication in connection with establishing and managing the IP addresses and domains used to operate the Shylock botnet. *FMAC Loan Receivables,* 228 F.R.D. at 534; *Rio Props., Inc. v. Rio Int'l Interlink*, 284 F.3d 1007, 1014-15 (9th Cir. 2002) ("[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…"); *BP Prods. N. Am., Inc. v. Dagra*, 236

F.R.D. 270, 271-273 (E.D. Va. 2005) (approving notice by publication in two Pakistani newspapers circulated in the defendant's last-known location); *Microsoft Corp. v. John Does 1-27,* Case No. 1:10-cv-156 (E.D. Va. 2010, Brinkema J.) at Dkt. 38, p. 4 (authorizing service by email and publication in similar action).

In this case, the e-mail addresses provided by Defendants to the hosting companies and domain registrars, in the course of obtaining services that support the botnet, are the most accurate and viable contact information and means of notice and service. Indeed, the physical addressees provided by Defendants to hosting companies 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 email and publication. *See BP Products North Am., Inc.,* 236 F.R.D. at 271. Moreover, Defendants will expect notice regarding their use of the hosting providers' and domain registrars' services to operate their botnet by e-mail, as Defendants agreed to such in their agreements with the service providers who provided the domains and IP addresses 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 locate Defendants, Due Process has been satisfied by Plaintiffs' service by publication and multiple email notices.

B. Default Judgment Is Appropriate

All of the relevant considerations point towards issuance of a default judgment against Defendants. *Compare Tweedy,* 611 F. Supp. 2d at 605-606 (applying default factors). First, the amount of money at stake weighs in favor of default judgment because Plaintiffs are not requesting any monetary relief, and indeed it is not possible for Plaintiffs 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. Plaintiffs have put forth a strong factual showing supported by expert testimony, forensic evidence, and documentary evidence from well renowned researchers who have studied the Shylock botnet 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 Shylock botnet violated the Computer Fraud and Abuse Act (18 U.S.C. § 1030); CAN-SPAM Act (15 U.S.C. § 7704); Electronic Communications Privacy Act (18 U.S.C. § 2701); the Lanham Act (15 U.S.C. § 1114 and § 1125(a) and (c)); and the common law of unjust enrichment, trespass to chattels, and conversion.

Third, this case involves a matter of substantial public importance. Defendants are perpetrating serious criminal offenses and civil torts that cause substantial harm to 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. Plaintiffs have made extraordinary efforts over the course of many months to ensure that Defendants were provided notice, and the evidence indicates that Defendants are actually or constructively aware of this action.

Fifth, Plaintiffs and other victims of the Shylock botnet 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 Plaintiffs 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. Plaintiffs Have Adequately Plead Each of Their Claims

The Complaint alleges that Plaintiffs have violated the Computer Fraud and Abuse Act (18 U.S.C. § 1030) ("CFAA"); Electronic Communications Privacy Act ("ECPA") (18 U.S.C. § 2701); trademark infringement under the Lanham Act (15 U.S.C. § 1114), false designation of origin under the Lanham Act (15 U.S.C. § 1125(a)); trademark dilution under the Lanham Act (15 U.S.C. § 1125(c)); and the common law of unjust enrichment, trespass to chattels, and conversion. 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). A "protected computer" is a computer "used in interstate or foreign commerce or communication." *E.g., SecureInfo Corp. v. Telos Corp.*, 387 F. Supp. 2d 593, 608 (E.D. Va. 2005). 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." *Id.* (citing 18 U.S.C. § 1030(e)(6)). In order to prosecute a civil claim under the CFAA, a plaintiff must demonstrate loss or damage in excess of $5,000.

The Complaint alleges that Defendants have surreptitiously accessed protected computers by infecting the computers with malware and then using the Shylock botnet infrastructure to control victim computers and to misappropriate personal information. Dkt. 1 at 19. Plaintiffs have provided evidence that they have suffered in excess of $5,000 dollars, and the Court credited this evidence in granting preliminary injunctive relief. *See* Dkt 33. Accordingly, Plaintiffs have properly alleged a CFAA claim and are entitled to default judgment on this claim.

Defendants conduct is precisely the type of activity the CFAA is designed to prevent. *See e.g. Penrose Computer Marketgroup, Inc. v. Camin*, 682 F. Supp. 2d 202 (N.D.N.Y. 2010); *Global Policy Partners, LLC v. Yessin*, 2009 U.S. Dist. LEXIS 112472, *9-13 (E.D. Va. 2009) (accessing computer using credentials that did not belong to defendant was actionable under the CFAA); *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).

ECPA Claim. The ECPA prohibits intentionally intercepting any electronic communication. *Global Policy Partners, LLC v. Yessin*, 686 F. Supp. 2d 631, 637 (E.D. Va. 2009) (citing 18 U.S.C. § 2511(1)(a)). Persons injured by violations of the ECPA may bring a civil suit to obtain injunctive relief and damages. *E.g., DIRECTV, Inc. v. Benson*, 333 F. Supp. 2d 440, 449 (M.D.N.C. 2004).

The Complaint alleges that the Shylock botnet intercepts communications while they are in transit, as well as while they are in storage, and that Defendants use personal information misappropriated from these intercepted communications to steal from victims and their banks. Dkt. 1 at 20. This conduct causes injury to FS-ISAC's member organizations (banks), and it also harms Microsoft's goodwill in its products. Accordingly, default judgment on Plaintiffs' ECPA claim is warranted. 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).

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. *E.g., George & Co., LLC, v. Imagination Entm't Ltd.*, 575 F.3d 383, 393 (4th Cir. 2009) (citing 15 U.S.C. § 1114(1)(a)). Here, the Complaint alleges that Defendants distribute

copies of Microsoft's registered, famous and distinctive trademarks in fraudulent versions of Defendants' Windows operating system and Internet Explorer browser, which deceive victims, causing them confusion and causing them to mistakenly associate Microsoft with this activity. Dkt. 1 at 20-22. Defendants similarly misuse the trademarks of FS-ISAC's third-party financial institutions as well. This conduct amounts to trademark infringement under section 1114. Defendants' conduct also constitutes false designation of origin under section 1125(a) and dilution by tarnishment, causing confusion and mistakes as to Plaintiffs' affiliation with Defendants' malicious conduct. *See, e.g., Brookfield Commc'ns.,* 174 F. 3d at 1066-67 (entering preliminary injunction under Lanham Act §1125(a) for infringement of trademark in software and website code).

Tort Claims. Under Virginia law, the tort of conversion "encompasses any wrongful exercise or assumption of authority . . . over another's goods, depriving him of their possession; and any act of dominion wrongfully exerted over property in denial of the owner's right, or inconsistent with it." *United Leasing Corp. v. Thrift Ins. Corp.*, 247 Va. 299, 305 (Va. 1994) (quotation omitted). The related tort of trespass to chattels applies where "personal property of another is used without authorization, but the conversion is not complete." *Dpr Inc. v. Dinsmore*, 82 Va. Cir. 451, 458 (Va. Cir. Ct. 2011) (citations omitted). Here, the complaint alleges that Defendants exercised dominion and authority over Microsoft's proprietary Windows and Internet Explorer software by injecting code into Microsoft's software that fundamentally changed important functions of the software, converted Plaintiffs' property including monies belonging to FS-ISAC member institutions, and were unjustly enriched with ill-gotten profits reaped from the Shylock botnet and its victims. Dkt. 1 at 24-26.

The well-pled allegations in Plaintiffs' Complaint, which set forth the elements of each of Plaintiffs claims, are taken as true given Defendants default. *SEC v. Lawbaugh*, 359 F. Supp. 2d 418, 421 (D. Md. 2005). Accordingly, the only question is what remedy to afford Plaintiffs.

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

In order to obtain a permanent injunction, a plaintiff must demonstrate: (1) that it has suffered an irreparable injury; (2) that remedies available at law, such as monetary damages, are inadequate to compensate for that injury; (3) that, considering the balance of hardships between the plaintiff and defendant, a remedy in equity is warranted; and (4) that the public interest would not be disserved by a permanent injunction. *E.g., EMI April Music, Inc. v. White*, 618 F. Supp. 2d 497, 509 (E.D. Va. 2009) (citing *Phelps & Associates, LLC v. Galloway*, 492 F.3d 532, 543 (4th Cir. 2007)).

1. Plaintiffs Have Suffered Irreparable Injury that Cannot be Compensated Monetarily

Consumer confusion and injury to business goodwill constitute irreparable harm. *See, e.g., Int'l Labor Mgmt. Corp. v. Perez*, 2014 U.S. Dist. LEXIS 57803, 35 (M.D.N.C. Apr. 25, 2014) (damage to "reputation and loss of goodwill constitutes irreparable harm for purposes of injunctive relief") (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 Plantiffs by the Shylock botnet constitutes irreparable harm. Dkt. 33 at 2. This finding is consistent with several cases that have concluded that the botnets 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.) (Ex Parte TRO to dismantle botnet command and control servers); *Microsoft v. Piatti, et al.*, Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.) (Ex Parte TRO and preliminary injunction

to dismantle botnet command and control servers); *Microsoft Corporation v. John Does 1-27*, Case No. 1:10-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.) (Ex Parte TRO and preliminary 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 irremediable absent an injunction because Defendants are elusive cybercriminals whom Plaintiffs are unlikely to be able to enforce judgments against. *See, e.g.*, *Khepera-Bey v. Santander Consumer 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 Overwhelmingly Favors an Injunction

Because Defendants are engaged in an illegal scheme to defraud consumers and injure Plaintiffs, the balance of equities clearly tips in favor granting an injunction. *See, e.g., US Airways, Inc. v. US Airline Pilots Ass'n*, 813 F. Supp. 2d 710, 736 (W.D.N.C. 2011); *Pesch v. First City Bank of Dallas*, 637 F. Supp. 1539, 1543 (N.D. Tex. 1986) (balance of hardships clearly favors injunction where enjoined activity is illegal). On one side of the scales of equity rests the harm to Plaintiffs and their customers caused by the Shylock botnets, while on the other side rests no legally cognizable harm to Defendants because an injunction would only require them to cease illegal activities. *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, such as the Lanham Act, CFAA, and ECPA. *See, e.g., 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); *accord Meineke Car Care Ctrs., Inc. v. Bica,* 2011 U.S. Dist. LEXIS 118171, 10 (W.D.N.C. Oct. 12, 2011) (similar); *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); *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).

Here, Plaintiffs request an injunction that will transfer permanent control of the botnet command and control domains to Microsoft. As a result, Microsoft can continue to assist victims in cleaning infected computers. Even for computers that cannot be cleaned, certain infected computers will be taken off line as they become obsolete or are replaced. Absent the requested injunction, the Shylock infrastructure will be released back into Defendants' control, and Defendants would be able to use that infrastructure to issue instructions to infected computers and to begin to revive and propagate the Shylock botnet. If this happens, Defendants can steal more personal information and commit more theft and fraud.

Given the risks the public will face absent an injunction, the calculus is clear. This is particularly so given that the requested injunction has been tailored only to the narrow scope of the uncontested injunction that has been in place since July 2014. 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 Microsoft's control of the botnet domains. In particular, the third-party domain registries responsible for administering the botnet 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 Microsoft at a domain

registrar to be designated by Microsoft. No additional steps are needed.

V. CONCLUSION

For all of the foregoing reasons, Plaintiffs respectfully request entry of default judgment pursuant to Rule 55(b) and a permanent injunction pursuant to Rule 65.

Dated: February 19, 2015 Respectfully submitted,

ORRICK, HERRINGTON & SUTCLIFFE LLP

/s/ David B. Smith

LAUREN J. PARKER
Va. State Bar No. 77018
DAVID B. SMITH
Va. State Bar No. 84462
Attorneys for Plaintiffs Microsoft Corp. and FS-ISAC, Inc.
ORRICK, HERRINGTON & SUTCLIFFE LLP
Columbia Center
1152 15th Street, N.W.
Washington, D.C. 20005-1706
Telephone: (202) 339-8400
Facsimile: (202) 339-8500
lparker@orrick.com
dsmith@orrick.com

Of counsel:

GABRIEL M. RAMSEY (admitted *pro hac vice*)
JACOB M. HEATH (admitted *pro hac vice*)
ROBERT URIARTE (admitted *pro hac vice*)
Attorneys for Plaintiffs Microsoft Corp. and FS-ISAC, Inc.
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401
gramsey@orrick.com
jheath@orrick.com
ruriarte@orrick.com