

Richard A. Jacobsen (RJ5136)
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, New York 10019
Telephone: (212) 506-5000
Facsimile: (212) 506-5151

Gabriel M. Ramsey (*pro hac vice*)
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, California 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

Attorneys for Plaintiffs
MICROSOFT CORPORATION,
FS-ISAC, INC. and NATIONAL AUTOMATED
CLEARING HOUSE ASSOCIATION

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK**

MICROSOFT CORP., FS-ISAC, INC., and
NATIONAL AUTOMATED CLEARING HOUSE
ASSOCIATION,

Plaintiffs

v.

JOHN DOES 1-21, 25-35 and 37-39,

Defendants.

Case No. 12-CV-1355 (SJ) (RLM)

MOTION TO AMEND PERMANENT INJUNCTION

Plaintiffs MICROSOFT CORP. (“Microsoft”), FINANCIAL SERVICES – INFORMATION SHARING AND ANALYSIS CENTER, INC. (“FS-ISAC”), and the NATIONAL AUTOMATED CLEARING HOUSE ASSOCIATION (“NACHA”) (collectively, “Plaintiffs”) respectfully move the Court pursuant to Federal Rule of Civil Procedure 60(b)(5) and 60(b)(6), Federal Rule of Civil Procedure 65, the All Writs Act (28 U.S.C. § 1651) and the court’s inherent equitable authority, to reopen the above-captioned case and to amend the permanent injunction issued by the court on December 5, 2012, addressing the Internet domains of the Defendants who operated and controlled the Zeus botnets. [Case No. 1:12-dv-1335-SJ-RLM, Dkt. 40 (12/5/2012)]

I. FACTUAL BACKGROUND

The Zeus botnets are estimated to have infected more than 13 million Internet users’ computers. (Complaint, Dkt. No. 1, ¶¶113, 116)¹ Through various fraudulent techniques such as spam e-mail purporting to be from legitimate organizations, including from Plaintiffs, innocent computer users are lured to websites from which malicious botnet code is surreptitiously installed on their computers. The botnet code then makes unauthorized changes to the infected computers and operating systems to bring the computer under the control of the botnet operators. The botnet code then waits for the unsuspecting user to attempt to connect to the website any one of a number of targeted financial institutions and to log into an account, during which time the botnet code captures the user’s account credentials. The botnet operators then use those credentials to steal money from the account or for other illegal purposes. (*Id.* ¶¶83-104)

On December 5, 2012, the Court entered a permanent injunction against the Defendants’ malicious operation of the Zeus botnets. (Dkt. 40, pp. 6-7) The permanent injunction also ordered third party domain registries, with administrative authority over the Internet domains used by Defendants to control the Zeus botnets, to redirect those domains to Microsoft’s secure servers for two years. (Dkt. 40, p. 7) The idea of this structure in the original permanent

¹ All docket numbers in the citations in this brief are to Case No. 1:12-dv-1335-SJ-RLM (EDNY).

injunction was that, in the two-year period, Microsoft would control the domains and take steps to clean up the infected computers attempting to connect to those domains. [Declaration of David Anselmi, ¶ 4] At the time, Microsoft believed that two years would be sufficient to clean up infected computers, after which the domains could be released by the registries to again be bought and sold on the open market. [*Id.* at ¶ 4] However, given the scale of the Zeus botnets, which historically has consisted of millions of infected computers, even today it is evident that there are tens of thousands of infected computers connecting to the domains and thus Microsoft needs the Zeus botnet domains transferred to its permanent ownership, such that it can exert longer term control over the domains, in order to continue clean-up efforts and mitigate the harm to its customers. [*Id.* at ¶ 5] Needing more than two years to mitigate the injury was unforeseen at the time that the original injunction was crafted. [*Id.* at ¶ 5] Also, if the domains were released at this time, given that there are still infected user computers connecting to them, it is possible that Defendants or associates of the Defendants could obtain the domains and continue the Zeus botnets' malicious activities. [*Id.* at ¶ 6]

None of the domain registries have objected to Microsoft's permanent ownership of the Zeus domains. [Declaration of Gabriel M. Ramsey, ¶¶ 2-4 (filed herewith).] One domain registry, Verisign, has indicated that it has no objection to transferring permanent ownership of the malicious Zeus domains to Microsoft, so that mitigation steps can continue, but takes the position that in the absence of a court order expressly authorizing it to do so, it can only comply with the terms of the original injunction (which ordered that the domains be redirected for two years and then released). [Ramsey Decl., ¶ 5] Accordingly, through this motion, Plaintiffs ask the Court to amend the permanent injunction to specifically authorize Verisign and other registries to transfer permanent ownership of the malicious Zeus domains to Microsoft.

A proposed amended permanent injunction is submitted with this motion and Plaintiffs seek entry of that amended permanent injunction. The only change from the prior permanent injunction is that the amended injunction specifically directs that the registries are authorized to

formally transfer the domains to Microsoft's ownership.² During the time that the injunction has been in place since 2012, no Defendant or any other party has come forward or otherwise taken issue with Microsoft having practical control over the Zeus botnet domains. [Ramsey Decl., ¶ 3]

II. LEGAL ANALYSIS

A Court that issues an injunction retains continuing jurisdiction to modify it whenever the principles of equity require it to do so. *United States v. United Shoe Machinery Corp.*, 391 U.S. 244, 248 (1968) (an injunction “may be changed upon an appropriate showing...”); *King-Seeley Thermos Co. v. Aladdin Industries, Inc.*, 418 F.2d 31, 34 (2d Cir. 1969) (same); *United States v. Am. Express Co.*, 2015 U.S. Dist. LEXIS 56945, *55 (E.D.N.Y. Apr. 30, 2015) (“if [parties] believe that the compliance provisions are unworkable, or require adjustments once implemented, they are permitted under the Permanent Injunction to seek modifications from the court.”). Injunctions may be modified to impose more stringent requirements to ensure the original purposes of the injunction are met. *Exxon Corp. v. Texas Motor Exchange of Houston, Inc.*, 628 F.2d 500, 503 (5th Cir. 1980). If the relief originally ordered has not produced the intended result, the Court “should modify the decree so as to achieve the required result with all appropriate expedition.” *United Shoe Machinery Corp.*, 391 U.S. at 252.

Similarly, under Federal Rule of Civil Procedure 60(b)(5), it is appropriate for a Court to reopen a case and revise an earlier injunction order where “applying it prospectively is no longer equitable.” Fed. R. Civ. P. 60(b)(5); *see also* Rule 60(b)(6) (authorizing case to reopened and prior orders revised for “any other reason that justifies relief.”); *Chepilko v. CIGNA Group Ins.*, 2011 U.S. Dist. LEXIS 20723, *16-17 (S.D.N.Y. Feb. 2, 2011) (re-opening case pursuant to Rule 60(b)(6)). In applying Rule 60(b)(5), district courts are to apply a “flexible standard.” *Rufo v. Inmates of Suffolk County Jail*, 502 U.S. 367, 381 (1992). A party seeking relief must show that changed circumstances warrant relief and, upon such showing, “a court abuses its discretion when it refuses to modify an injunction or consent decree in light of such changes.” *Id.* (internal

² The modified terms are located at Pages 6-7 of the Proposed Amended Permanent Injunction, submitted with this motion, in Section “H.”

citations omitted); *Calderon v. Wambua*, 2012 U.S. Dist. LEXIS 46193, *8-11 (S.D.N.Y. Mar. 28, 2012) (same, modifying injunction).³ A change in factual conditions such as “a decree [that] proves to be unworkable because of unforeseen obstacles” or “enforcement of the decree without modification would be detrimental to the public interest.” *Id.* If so, the Court may enter modifications “suitably tailored to the changed circumstance.” *Id.*

Modification of an injunction is particularly appropriate here, where the Defendants’ activities have caused ongoing injury in the form of millions of infected computers, the continued existence of which frustrates the purpose of the original injunction’s terms. The original relief, which redirected the botnet domains for only two years, has not yet produced the intended result. In sum, Microsoft needs longer term ownership and control over the botnet domains, in order to clean up the massive number of computer infected by Defendants. Thus, given the unforeseen obstacles that render the prior injunction unworkable, there is a significant change in factual conditions that makes it appropriate to modify the injunction pursuant to Rule 60(b)(5) and the Court’s equitable powers. Likewise, the terms of the current injunction, which would allow the still-active botnet domains to be released after two years, and would allow Defendants to re-exert control over the botnets would be detrimental to the public interest. For this reason as well, amendment of the permanent injunction is appropriate under Rule 60(b)(5) and the Court’s equitable authority. The modified injunction is narrowly tailored such that the relief granted is not substantively any different than the relief previously granted in the original

³ The proposition that a court has the authority to alter the prospective effect of an injunction in light of changes in circumstances is well-established. *See, e.g., System Federation No. 91, Railway Employees' Department, AFL-CIO v. Wright*, 364 U.S. 642, 647 (1961) (“The source of the power to modify is of course the fact that an injunction often requires continuing supervision by the issuing court and always a continuing willingness to apply its powers and processes on behalf of the party who obtained that equitable relief.”); *United States v. Swift & Co.*, 286 U.S. 106 (1932) (“The power of a court of equity to modify an injunction in adaptation to changed conditions” is “inherent in the jurisdiction of the chancery. A continuing decree of injunction directed to events to come is subject always to adaptation as events may shape the need.”); *Chrysler Corp. v. United States*, 316 U.S. 556, 562 (1942); *Agostini v. Felton*, 521 U.S. 203, 117 S. Ct. 1997 (1997) (“A court errs when it refuses to modify an injunction or consent decree in light of changes.”).

injunction, but rather simply transfers the botnet domains to Microsoft permanently, so that Microsoft has sufficient time to clean up victim computers and achieve the purposes of the injunction. *See e.g. United Shoe Machinery Corp.*, 391 U.S. at 252; *Rufo*, 502 U.S. at 381 (1992); *Calderon*, 2012 U.S. Dist. LEXIS 46193 at *8-11.

Courts have transferred ownership of harmful domains where prior injunctive measures did not sufficiently mitigate the injury caused by the domains. For example, in *Philip Morris USA, Inc. v. Otamedia Ltd.*, 331 F. Supp. 2d 228 (S.D.N.Y. 2004), the court enjoined the defendant's unauthorized sale of Philip Morris cigarettes over the Internet, which constituted trademark infringement. Philip Morris then requested the court modify the injunction, asking the court for the transfer to Philip Morris ownership of certain Internet domain names through which defendant continued to violate the injunction. *Id.* at 229. The court granted the motion and modified the injunction, stating a “[c]ourt’s paramount obligation must be to ensure compliance with [prior] [j]udgment[s].” *Id.* at 245. The court recognized that transfer of the domain names would be “an efficacious means to enforce the Judgment, a means inherent in the very same technology by which [defendant] has to date been able to violate it with impunity.” *Id.* The court also noted that where the injunction's beneficiary seeks to enforce it more effectively, “equity countenances the modification of an injunctive decree if ‘a better appreciation of the facts in light of experience indicates that the decree is not properly adapted to accomplishing its purposes.’” *Id.* at 244 (citing *Sizzler Family Steak Houses v. W. Sizzlin Steak House, Inc.*, 793 F.2d 1529, 1538-40 (11th Cir.1986).)

In view of the foregoing, Plaintiffs submit that modification of the Court’s Permanent Injunction to include authorization for the domain registries to permanently transfer control of the Zeus botnet domains to Microsoft is an appropriate, just means by which to ensure that the injury to consumers and to Microsoft caused by the Defendants can be mitigated and that Defendants are not able to re-exert control over the Zeus botnets. As a practical matter, the proposed amendments to the permanent injunction have the same result as the prior injunction—i.e. Microsoft will control the Zeus botnet domains and be able to use them to clean up infected

computers—but the amendments continue that situation into the future by transferring permanent control to Microsoft. The requested modification is particularly appropriate, given that it is not objected to and, indeed, encouraged by the third-party domains registries who are willing to permanently transfer Defendants’ domains to Microsoft, but do not believe they can act unilaterally, given the terms of the prior injunction. Moreover, there is no burden on any third party, Microsoft will pay for the administration and registration of the domains, once transferred to Microsoft’s control.

III. CONCLUSION

WHEREFORE, Plaintiffs respectfully request that this Court grant their Motion to Amend the Permanent Injunction in the form filed herewith, in order to transfer ownership of the Zeus botnet domains to Microsoft.

Dated: June 17, 2015
New York, New York

Respectfully Submitted,

ORRICK, HERRINGTON & SUTCLIFFE LLP

By: s/ Gabriel M. Ramsey
Gabriel M. Ramsey (*pro hac vice*)
1000 Marsh Road
Menlo Park, California 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401
gramsey@orrick.com

Richard A. Jacobsen
51 West 52nd Street
New York, NY 10019
Tel: (212) 506-5000
Fax: (212) 506-5151
rjacobsen@orrick.com

Attorneys for Plaintiffs
Microsoft Corporation
National Automated Clearing House Association
FS-ISAC, Inc.