

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
(admitted *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.

Hon. Sterling Johnson, Jr.

Case No. 12-cv-01335 (SJ/RLM)

**DECLARATION OF DAVID ANSEMI
IN SUPPORT OF MOTION TO AMEND PERMANENT INJUNCTION**

I, David Anselmi, declare as follows:

1. I am a Senior Investigator in the Digital Crimes Unit of Microsoft Corporation's Legal and Corporate Affairs Group. I make this declaration in support of Plaintiffs Motion to Amend Permanent Injunction. I make this declaration of my own personal knowledge and, if called as a witness, I could and would testify competently to the truth of the matters set forth herein.

2. In my current role at Microsoft, I assess technical security threats to Microsoft and the impact of such threats on Microsoft's business and customers. Prior to my current role, I worked as Senior Technologist, dealing with security of Microsoft's online services. Among my responsibilities were protecting Microsoft online service assets from network-based attacks. Prior to that, while also employed by Microsoft, I worked as a Senior Technologist, dealing with protecting Microsoft's corporate resources from network-based attacks. Before joining Microsoft, I worked for Excell Data Corporation as a Program Manager performing security firewall deployment, configuration, and administration. I am a graduate of the United States Military Academy, West Point, and served for 27 years as a United States Army Communications Electronics Officer (11 years active, 16 reserve), attaining the rank of Lieutenant Colonel.

3. On December 5, 2012, the Court entered a permanent injunction against the Defendants' malicious operation of the Zeus botnets. 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.

4. The reason for the structure in the original permanent injunction was that it was believed that, during the two-year period, Microsoft would control the domains and take steps to clean up the infected computers attempting to connect to those domains. 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.

5. 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. It was unforeseen at the time that the original injunction was crafted that Microsoft would need more than two years of control over the domains to mitigate the injury. At this point, it is evident that the terms of the existing permanent injunction are unworkable, given the unforeseen obstacle that there would continue to be many infected computers attempting to connect to the domains. The simplest, most efficient and effective way to craft effective relief is to simply transfer ownership of the domains permanently to Microsoft. This is also the least burdensome for the domain ecosystem and the domain registries and registrars, because those entities will need to do nothing beyond their normal business operations and Microsoft will own and pay for the domains.

6. If the Zeus botnet domains were released at this time by the domain registries, as contemplated by the original permanent injunction, given that there are still many infected user computers connecting to those domains, it is possible that Defendants or associates of the Defendants could obtain the domains on the open market and use them to resurrect the Zeus botnets and continue the malicious activities that are enjoined by the permanent injunction. This would cause injury to Plaintiffs and the end-user customers, precisely of the type that the permanent injunction is intended to prevent.

7. By transferring permanent ownership of the Zeus botnet domains to Microsoft, as set forth in the proposed amended permanent injunction, the risks posed to consumers by their infected computers and the risks posed by Defendants regaining control of the botnets will be diminished substantially.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed this 20th day of May, 2015.

A handwritten signature in cursive script that reads "David E Anselmi".

David Anselmi