Additional Comments on Improper Zango Practices

Ben Edelman and Eric Howes

December 3, 2006

Last month we submitted comments regarding the FTC's proposed settlement with Zango, Inc. We flagged numerous ongoing installations that, in our judgment, show Zango in violation of the terms of the settlement –raising serious questions about "the efficacy and viability of the FTC's proposed settlement as well as Zango's ability to meet the requirements of the settlement." Since we submitted our original set of comments, other disturbing Zango installations have come to light. These new Zango installations are predicated on deceptive practices involving a MySpace worm which, in addition to seizing users' MySpace passwords, also sends users to web pages hosting videos that install Zango's software (through the deceptive license acquisition process that we previously critiqued).

These new Zango installs are disturbing not because they put Zango in violation of the terms of proposed settlement, but precisely because they do not -- because these installations, disturbing though they may be, do not clearly violate any of the settlement's requirements. Inasmuch as these new installations are not in direct violation of the settlement's terms, they raise the alarming prospect that this settlement could allow Zango to continue to pay distributors to create malicious and/or deceptive software and web pages.

The MySpace Worm & Zango Installs

Numerous reports confirm large numbers of MySpace seeing their MySpace profiles compromised by a JavaScript worm. Analysis confirmed that the worm spreads from infected MySpace profiles to the profiles of other users who happen to visit infected profiles or who include those infected profiles in their own MySpace "Friends" lists. References:

> GhettoWebMaster. "MySpace Worm: Phishing Accounts and Spreading Zango Porn."
> http://www.ghettowebmaster.com/code/myspace-phishing-zango-porn-worm/
>
> SpywareGuide.com (Facetime). "Myspace Phish Attack Leads Users to Zango Content."
> http://blog.spywareguide.com/2006/12/myspace_phish_attack_leads_use.html
>
> Paperghost. "Phishing attack on Myspace leads to....Zango videos."
> http://www.vitalsecurity.org/2006/12/phishing-attack-on-myspace-leads.html
>
> F-Secure. "New Myspace worm using a Quicktime exploit."
> http://www.f-secure.com/weblog/archives/archive-122006.html#00001038

These practices are remarkably deceptive. The worm uses a QuickTime feature to overlay injected links to fake login forms ("phishes") that appear to come from MySpace itself. Furthermore, the worm sends spam directing recipients to a site hosting pornographic videos that attempt to install Zango's software through the deceptive "license acquisition" process we previously described.

Implications of These Deceptive Installations on Zango's Practices and the Proposed FTC Settlement

These deceptive installations crisply present a serious question of FTC policy: May Zango continue to receive installations predicated on user deception, if those installations satisfy the notice and consent procedure set out in the proposed settlement?

We think such installations ought not be permitted. We think consumers cannot grant meaningful, informed consent when an installation is predicated on a worm or a phish. Furthermore, we think consumers cannot grant meaningful consent when installation is solicited by pretending to be an authorized banner advertiser on Google (as in our prior comment's Section G spyware injection example) or by pretending to be Youtube (as in our Section G typosquatter example).

Yet we anticipate that Zango will argue that any installs perpetrated through this MySpace scheme (or the Section G examples we previously documented) are legitimate and permissible because Zango's S3 screen was displayed, containing required notice and disclosure text. Zango will claim that even if consumers were directed to the Zango-sponsored videos through deceptive means, that deception was cured by the presence of the S3 screen. We worry that the proposed settlement does little to prevent such an argument and, indeed, effectively endorses it.

We believe the FTC's proposed settlement with Zango is fatally flawed because it fails to address these deceptive Zango installs -- installs that lie at the heart of ongoing deceptive installations of Zango's software. We think a cure to this defect lies in prior FTC caselaw, namely the "deceptive door opener" line of cases (e.g. *Federal Trade Commission v. Encyclopaedia Britannica*, Inc., 87 F.T.C. 421 (1976)). We think these cases are squarely on point. Where Zango's initial contact with a consumer occurs through deception, as set out above, we think the deception cannot be cured. We think the FTC could appropriately add language to that effect to its proposed settlement with Zango – reiterating that materially deceptive installations, by Zango or by its distributors, cannot be corrected merely through the notice and consent procedure otherwise set out in the proposed settlement.

More generally, we continue to doubt that Zango can supervise its distributors ("affiliates") with sufficient rigor to assure that distributors' practices are honest, ethical, and appropriate. If Zango cannot adequately supervise its distributors, the FTC may have no choice but to insist that Zango cease operating through distributors.

Finally, so long as these deceptive installations continue, we believe further monetary penalties are needed. Zango ought not retain whatever profits it earned from these deceptive installations. We think the FTC should require Zango to disgorge all such profits, and to forfeit these improper installations (via automatic uninstallation of all Zango software that was installed improperly).