FROM: Jay Huie

The largest issue I see with the proposed solution is that it only outlines the 'green path' approach, i.e. what happens if a bot is successfully detected, if the customer successfully mitigates the threat (by following the link to a resolution) and if the path /dis-infectant successfully completes.

However, this idealized version of reality avoids some critical components;

(1) What happens if a customer's machine is mistakenly placed into an 'infected' category?
In this case the solution effectively denies them an "inalienable right" (as Internet Access has been defined in some circles).

(2) What happens if the customer does not want to disable the bot (perhaps they are a security researcher)
In this case there are ethical concerns with both (a) permitting access or (b) continuing to deny access

(3) What happens if the clean-up solution fails?
Who is liable if the supposed mitigation actually ends up wiping a machine?

(4) How can consumers be certain they are executing an approved solution, and haven't been maliciously routed to a trojan site that causes them to install an even worse infection?

In short the idea has some promise although I believe it ultimately has more issues than can reasonably be dealt with, particularly given the implications of FCC's net-neutrality rules.