I am responding as a private citizen.

As far as I know, the State of Virginia is unique among governments organizations that, using existing alert channels, notifies affected Virginia citizens or organizations of the possibility that their computer has been infected with malicious software.

http://www.vita.virginia.gov/uploadedfiles/VITA_Main_Public/unmanaged/security/information_security_awareness_month/2007/Keylogging_Letter.pdf

In addition to enlisting ISPs and others in this effort, I believe that the US-CERT currently shares such information with a large number of federal and state organizations, but then leaves it up to the receiving organization to do something, anything, to address the problem. This approach is not working.

I propose that US-CERT and the FTC (which has evolved into a consumer focused site for dealing with the impact of identity theft) together work on a way to identify the affected citizen or organization, (or at least provide this information to their ISP) and send a letter similar to the one used by Virginia to alert the citizen of the problem. I recognize that often the US-CERT gets their information from sources that are not attributable but which are valid, and rather than have a couple hundred federal and/or state agencies all ding their own thing (if they are doing anything at all) having these two take the lead would put some muscle behind this.

It's simply immoral for the government to know that a citizen has an infection on their computer and NOT try and tell them about it. It's a parallel to our views on fighting STDs, we need to let people know that they are infected so that they can take steps to get clean. Knowing that someone is infected but doesn't know it is not what we expect the government to do.

I may not expect them to fix the problem for me, but getting told I have a problem is fair enough.

John McGing