

Re: A 6% fix from Microsoft Security Bulletin MS03-040 – 828750

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2003-10/0838.html>

From: Me2 (nospam_at_nospam.com)

Date: 10/05/03

Date: Sat, 4 Oct 2003 21:23:00 -0700

Rob,

Yes, I did take it that you somehow were reducing the seriousness of the Trojan.QHosts one of our executives got installed on his PC. I need to tell you that I am (was?) a M\$ advocate in that we have a vast investment in M\$ software. We has spend tons of money on security (firewalls, DMZ, monitoring, proxies, anti-virus, email monitors, etc) and what does it take to have your information compromised? Just visiting a site with IE 6 (with the most current patches and AV installed) – the site that you visit could be one that you have visited before and is deemed ok. But the site uses advertising banners from a third party – and today one of the little ad banners is able to change the registry, add, delete and modify files. WOW, is that a problem or what? And you know what M\$ was telling us about this bug – NOTHING!!!

You know what M\$ told me when I called about the Trojan.QHosts infection – sorry its not our problem (in a lot more words) – see your AV vendor!!! Then nearly on the same day I find news articles all over the place talking about the Qhosts and how M\$ does not have a fix yet. Some of the articles refer to the 31 holes in IE. 31 un-patched vulnerabilities!!! So when MS03-040 is released – does M\$ tell us that it fixed the hole that Trojan.Qhosts used? NO, I need to find out on a new group or in the media.

Getting back to your question:

- > *"If Microsoft and the antivirus companies made*
- > *as big a fuss about even the trivial stuff as they do about the serious*
- > *stuff, do you think that would heighten awareness? Or would it be more*
- > *likely to confuse people and cause them to "switch off" and not listen to*
- > *the warnings?"*

Big fuss? First of all M\$ has ZERO information about Trojan.QHosts. They only make a big fuss about the release of a fix!!! (or a bug that is effecting millions) Seems to be a complete lack of empathy for their customers who are experiencing serious security breaches because of their products. No information – let that sink in – M\$ is not telling us about problems (i.e. Trojans/viruses/worms) that are effecting the security of

their products!!! What total arrogance!

I agree that there are different levels risks and fix priorities that need to be assigned but that is different than providing ZERO information. Yes, I guess that M\$ should only release a "news alert" about a new virus/worm/Trojan if there are over X number of people and organizations effected. What do you suggest for this X number? 1000, 10000, 1K, 1 million or more PCs infected and information compromised? Just look at the masses of junk mail from swen – boy M\$ will be really liked if there is another virus infecting another 10000+ PCs on the net spewing out more junk emails.

Sorry, if I sound mad – I am – I can't get over that M\$ would not be warning their customers about potential vulnerabilities in their products – they are likely working on the next fixes – but we are left to suffer because M\$ is arrogantly not warning their customers about vulnerabilities. We don't need any of the technical details, just some recommendations on risks and tradeoffs of using IE or other products.

Seems to me that if M\$ had at least warned (no news release – just a post/recommendation on their security pages) about the IE vulnerabilities, customers could decide FOR THEM SELFS if it is worth the risk of allowing Internet IE browsing from within a corporation. Maybe we need to setup a separate network for Internet browsing until M\$ gets things under control – I don't know. Home users are certainly on their own when it comes to information security.

I hope to God that the Department of Homeland Security is not open to the Internet!!!

Thanks, for talking. I just kinda needed an outlet.
Me

> > *Rhetorical questions: Why doesn't Microsoft post information about
> > current Trojans/viruses/worms like Trojan.Qhosts???* Does it take
> > *hundreds of thousands or millions of infections to warrant a note???*
> > *Is thousands (or tens of thousands) not merely enough???* The
> > *www.microsoft.com/security page "Technical Virus Alerts" lists a
> > massive 26 entries from Nov 26 2001 (badtrans) through Sep 18 2003
> > (swen). Does the Trojan.Qhosts warrant a fix (ms03-040) but not an
> > entry on this list?*
>
> *Good question. Even with the purchase of RAV, Microsoft obviously don't
see
> themselves currently as in the antivirus business. There are several
viruses
> and the like "discovered" daily.. yes every day, and even those companies
> that are in the antivirus business don't make a big song and dance about
any
> except those they think are going to be a serious problem.*
>

> *Leaving aside QHosts specifically for the moment, and asking a general*
> *question of my own, if I may. If Microsoft and the antivirus companies*
made
> *as big a fuss about even the trivial stuff as they do about the serious*
> *stuff, do you think that would heighten awareness? Or would it be more*
> *likely to confuse people and cause them to "switch off" and not listen to*
> *the warnings?*
>
> *I suspect there isn't a single "right" answer to that question.*
>
>
> *Regards,*
> --
> --
> *Rob*
> *Microsoft MVP*
> *Windows Servers and Security*
> <http://www.robertmoir.co.uk>
>