

Re: HijackThis Log Help

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2007-12/msg01145.html>

- *From:* "Michael Jenkin [SBS-MVP]" <michael.jenkin@xxxxxxxx>
 - *Date:* Sat, 08 Dec 2007 10:48:35 +1000
-

I agree. I never could certify a machine clean. If I see a rootkit, I almost always suggest a reformat even if it took me seconds to discover the rootkit. If it is normal Spyware, I try and clean it up.

All my clients are SBS 2003 Premium (With ISA), have restrictive access to websites with known malware on them (And we have url scanning activated), do not have access to their local registry or control panels (By Policy) are given strict instructions not to download suspicious things and they run Trend Neatsuite + Antispyware. They are as protected as I can make them.

They still get some form of infection at a rate of 1 user a day. (I have lots of clients and lots of machines to look after. I have about 80 SBS installs live on my books (I have lots more but they now have their own internal person doing basic IT now) with an average of 30 pc's per install – i.e thousands of end users). I work in some high risk business like trucking and mining. These guys love the wrong kinds of websites.

If I look at the number of new servers we do per month (About 2 a month with all new workstations) and the number of new PC's the existing 80 or so clients buy, then the backups that occasionally fail, the power failures, other items client need and the help they need with new software, I really do not have the resources to be reformatting every PC and reinstalling all their Apps. The client normally does not want that kind of downtime. Sometimes repair is the faster option.

I have seen enough infections now to get a gut feel when to reformat or when to battle it out. I have numerous tools and I cross check everything. I also follow the clients up afterwards and keep an eye on them and if their machines are trying to make anonymous connections to the internet etc.

So ... I agree. I can't certify. To date though, I have repaired more pc's than I have reformatted. I do not recall any PC playing up again in the following months so I feel my success rate and caution has been good.

I leave the machines in good hands with Trend micro and all the other

Re: HijackThis Log Help

security.

Leythos wrote:

In article <utz8fpFOIHA.5160@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>, michael.jenkin@xxxxxxx says...

I weigh the time of a reformat, reinstall, reinstall all drivers and applications and put back any missing settings against Malware removal time which at the most takes me about 1 hour actual hands on. Items like trend Housecall etc can run longer than 1 hour so I do them overnight.

But, while repair is minimal, there is still risk that you didn't get it all. You can not possibly be 100.00% certain you actually removed all malware vs what a wipe/reinstall would provide them.

When it comes to "Certifying" that a computer is clean, I will not provide my signature unless I've wiped it and reinstalled it in a clean environment.

I've never found any ethical person that could suggest, 100.00%, that they could clean a compromised machine.

—

Michael J. Jenkin MVP – SBS, MCP, Small Business Specialist, Senior Systems Engineer
Visit <http://www.mickyj.com>

.