

Forum:[Hack Forums](#)

Thread: [MWB Blocking connections to svchost.exe](#)

001001 - December 24, 2014, 11:04 pm

Hey I am not sure if I am infected but I am experiencing things I have not before.

I own MWB and have the live web blocking on and am getting connections to svchost.exe being blocked. Plus there has been a few times that it looked like a program has opened and closed really fast. Things are also going a little slower.

Quick/Threat scan finds nothing.

Code Malicious Website Protection, IP, 93.190.109.37, 59243, Inbound,
C:\Windows\System32\svchost.exe,
Malicious Website Protection, IP, 93.190.109.37, 59243, Inbound,
C:\Windows\System32\svchost.exe,
Protection, Malicious Website Protection, IP, 93.190.109.37, 59243, Inbound,
C:\Windows\System32\svchost.exe,

Aura - December 24, 2014, 11:06 pm

Malwarebytes Web Protection module is known to throw a lot of false positives on processes like svchost.exe, chrome.exe, skype.exe, utorrent.exe. The best thing to do is to ignore it or simply disable it and leave web protection in the hand of your Antivirus product and your Firewall. This is the 10,000th thread on the subject here. Thread closed.

Null Byte - December 25, 2014, 5:39 pm

Do you have any Russian software? Because the IP belongs to a Russian company called Sibirskie Seti Ltd. I think we should do a checkup for malware if it's ok with you.

001001 - December 25, 2014, 7:25 pm

Yea I don't have any Russian software that I know of.

Aura - December 25, 2014, 7:44 pm

(Dec 25, 2014 08:25 PM)001001 Wrote: [\[CITE\]](#) Yea I don't have any Russian software that I know of. What are you doing exactly on your system when that connection is being prompted?

001001 - December 25, 2014, 8:39 pm

(Dec 25, 2014 08:44 PM)Aur? Wrote: [\[CITE\]](#) What are you doing exactly on your system when that connection is being prompted?

That has happened during watching a movie, browsing online, playing a steat game. Nothing that I at the moment can think of is common to each time I've seen it pop up.

Aura - December 25, 2014, 8:41 pm

(Dec 25, 2014 09:39 PM)001001 Wrote: [\[CITE\]](#) That has happened during watching a movie, browsing online, playing a steat game. Nothing that I at the moment can think of is common to each time I've seen it pop up.

To be honest, just the "browsing online" could have triggered that alert if you were on a website that loads content from a Russian server or else. It's way too vague to see if you're indeed infected or not. Does Malwarebytes detects anything with a Threat Scan?

001001 - December 25, 2014, 8:52 pm

No it does not. It has happened with nothing opened and an idle PC while I was watching tv.

Aura - December 25, 2014, 8:53 pm

(Dec 25, 2014 09:52 PM)001001 Wrote: [\[CITE\]](#) No it does not. It has happened with nothing opened and an idle PC while I was watching tv.

Then it's caused by a background process or service running. What services do you have running under svchost.exe?

jonas99 - December 29, 2014, 3:05 pm

Russians trying to hack you... scan your pc :) Antivirus :)

Aura - December 29, 2014, 3:06 pm

(Dec 29, 2014 04:05 PM)jonas99 Wrote: [\[CITE\]](#) Russians trying to hack you... scan your pc :) Antivirus :)

Stop fucking shitposting in this section.

001001 - December 29, 2014, 9:11 pm

I have quite a few running, like 7 svchosts. Looked like audio software. I have the firewall and av, is there and up to date. You say it should be fine then I will assume I was wrong.

Aura - December 29, 2014, 9:12 pm

(Dec 29, 2014 10:11 PM)001001 Wrote: [\[CITE\]](#) I have quite a few running, like 7 svchosts. Looked like audio software. I have the firewall and av, is there and up to date. You say it should be fine then I will assume I was wrong.

For me you're fine, since a single connection doesn't prove anything. What if one of the background service updates from a server in Russia. Even if the possibility is low, it still is possible. Without any concrete detections or logs, there's not much that we can do.

001001 - December 29, 2014, 9:19 pm

(Dec 29, 2014 10:12 PM)Aur? Wrote: [\[CITE\]](#) For me you're fine, since a single connection doesn't prove anything. What if one of the background service updates from a server in Russia. Even if the possibility is low, it still is possible. Without any concrete detections or logs, there's not much that we can do.

There are other ip's that it blocks but nothing has been tampered with or logged under other ip's. Did pass changes and such. No threats as of the first post as well.

Aura - December 29, 2014, 9:21 pm

(Dec 29, 2014 10:19 PM)001001 Wrote: [\[CITE\]](#) There are other ip's that it blocks but nothing has been tampered with or logged under other ip's. Did pass changes and such. No threats as of the first post as well.

I would leave all the web protection/traffic in the hands of your Antivirus product/Firewall. Malwarebytes classify as "suspicious" IP addresses it doesn't know.

001001 - December 29, 2014, 9:22 pm

(Dec 29, 2014 10:21 PM)Aur? Wrote: [\[CITE\]](#) I would leave all the web protection/traffic in the hands of your Antivirus product/Firewall. Malwarebytes classify as "suspicious" IP addresses it doesn't know.

Oh yea I let them all run. Thank you a lot by the way.

Aura - December 29, 2014, 9:32 pm

(Dec 29, 2014 10:22 PM)001001 Wrote: [\[CITE\]](#) Oh yea I let them all run. Thank you a lot by the way. No problem, glad that I could be of assistance.

