

Forum:[Hack Forums](#)

Thread: [Hitman Pro classifies svchost as suspicious...](#)

James Burnham - April 23, 2017, 11:20 am

What should I do? It gives me the option to replace or ignore. Uploading it on virustotal gives that <https://www.virustotal.com/el/file/710134ffaf3a08d1b217da2f90afd85ae2e0d20f5d8968901b5943b26aa2f44b/analysis/1492941215/>

DaFriendlySentry - April 23, 2017, 1:57 pm

Probably a rootkit? (Programs that disguise themselves as a legit windows program or something)

Travelers - April 23, 2017, 3:10 pm

Do you have any reason to believe that this is something malicious? Are you noticing craziness on your system?

James Burnham - April 23, 2017, 3:23 pm

(Apr 23, 2017 03:10 PM)proxyrhythmic Wrote: [\[CITE\]](#) Do you have any reason to believe that this is something malicious? Are you noticing craziness on your system?

No I don't notice anything weird on my system. The only reason I believe it may be malicious is because it showed up on Hitman Pro.

Travelers - April 23, 2017, 3:28 pm

I see that you could go two ways with this:

- 1) It's a false positive. Nothing to see here, folks.
- 2) Pursue it; dive down the rabbit hole. Crack open process explorer and give it a look over. Have process monitor open at system start up, let it run for a few minutes, stop it then review. See if anything was opened or leads you to think there is anything going on. Deep dive, so to speak.

This is what I would do, anyway. Hope this helps.

JoshuTee - April 23, 2017, 4:05 pm

This certainly is very suspicious. It's not signed by Microsoft but masquerades as a system file. It even contains the string "PAYLOAD".

Please boot into safe mode and use Autoruns to find the file location, and delete it.

Travelers - April 23, 2017, 6:45 pm

Let us know what you find. I would seriously suggest combining what I stated as well as JoshuTee. Vouching for him. Seen him around and he's smartly. ?

Soulmate~?? - April 23, 2017, 6:47 pm

I usually show these to people who think their svchost is infected.

<https://hackforums.net/showthread.php?tid=5562389&pid=54319032#pid54319032>
<https://hackforums.net/showthread.php?tid=5556187&pid=54147490#pid54147490>

Travelers - April 24, 2017, 3:18 am

(Apr 23, 2017 06:47 PM)Soulmate~?? Wrote: [\[CITE\]](#) I usually show these to people who think their svchost is infected.

<https://hackforums.net/showthread.php?tid=5562389&pid=54319032#pid54319032>
<https://hackforums.net/showthread.php?tid=5556187&pid=54147490#pid54147490>

Both seem to be very good resources. I'll be bookmarking these two threads ?

JoshuTee - April 24, 2017, 7:12 am

(Apr 23, 2017 06:47 PM)Soulmate~?? Wrote: [\[CITE\]](#) I usually show these to people who think their svchost is infected.

<https://hackforums.net/showthread.php?tid=5562389&pid=54319032#pid54319032>

<https://hackforums.net/showthread.php?tid=5556187&pid=54147490#pid54147490>

This is not very accurate to be honest. It's true for most cases but svchost.exe may also exist in C:\Windows\sysWoW64 or a subfolder of C:\Windows\WinSxS.

Having that said it can also be that the instance of svchost running has been injected with malicious code or has been infected with a virus.

Generally it's much safer and easier to check for certificates. Every svchost.exe that belongs to Windows has a valid Microsoft certificate. If it does not, it is almost certainly counterfeit.

GruntStyl - April 25, 2017, 9:33 am

(Apr 23, 2017 04:05 PM)JoshuTee Wrote: [\[CITE\]](#) It's not signed by Microsoft Looks signed to me? Unless were looking at two different VT links.

Could just be a false positive from HitmanPro seeing as 60 other antiviruses don't flag it as suspicious. According to VirusTotal the file is Digitally signed by Microsoft so it is a Microsoft process. However that doesn't mean another application hasn't "binded"/"Injected" it's self into the process in memory. In which case Virustotal wouldn't detect it anyways as your just uploading the file it's self and nothing associated with it.

If it were me in this situation I'd just use a utility like process explorer and see if anything looks suspicious with the process and go from there.

JoshuTee - April 25, 2017, 9:57 am

(Apr 25, 2017 09:33 AM)Tazzy0pz Wrote: [\[CITE\]](#) Looks signed to me? Unless were looking at two different VT links.

Oh. You're right. My mistake!

James Burnham - April 25, 2017, 1:17 pm

I am sure I had seen it as "unsigned". I don't know why now it says it is signed.

JoshuTee - April 25, 2017, 3:10 pm

(Apr 25, 2017 01:17 PM)Mr. Burnham Wrote: [\[CITE\]](#) I am sure I had seen it as "unsigned". I don't know why now it says it is signed.

Me too to be honest. I was absolutely sure.

Anyway I'm trying to get my hands on the actual file now.

Hackoo - April 25, 2017, 3:44 pm

Hi ?

You can download [System Explorer](#)

This small software includes many usefull tools which help you Keep Your System Under Control . With System Explorer You get also fast access to File Database which help you to determine unwanted processes or threats.

Main Features :Detailed information about Tasks, Processes, Modules, Startups, IE Addons, Uninstallers, Windows, Services, Drivers, Connections and Opened Files.

Easy check of suspicious files via File Database or the VirusTotal service.

Easy monitoring of processes activities and System changes.

Usage graphs of important System resources.

Tray Hint with detailed System and Battery status.

WMI Browser and System Additional Info

Multilanguage Support