

Forum:[Hack Forums](#)

Thread: [CPU is high untill i open taskmanager...](#)

IS-14 - October 24, 2017, 2:25 am

My cpu is so high and when i open taskmanager it goes back down quickly to like 2,3%...

GGWP1337 - October 24, 2017, 5:39 am

What are you doing when this issue occur?

Smile? - October 24, 2017, 5:43 am

Silent miner probably , check your processes from cmd.

IS-14 - October 24, 2017, 9:35 am

(Oct 24, 2017 05:43 AM)?dâFu™ Wrote: [\[CITE\]](#) Silent miner probably , check your processes from cmd.

Microsoft Windows [Version 10.0.15063]

© 2017 Microsoft Corporation. All rights reserved.

C:\Users\tsach>tasklist

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	8 K
System	4	Services	0	23,112 K
smss.exe	424	Services	0	1,008 K
csrss.exe	620	Services	0	4,376 K
wininit.exe	720	Services	0	5,212 K
csrss.exe	736	Console	1	4,696 K
winlogon.exe	824	Console	1	17,696 K
services.exe	944	Services	0	8,360 K
lsass.exe	952	Services	0	45,616 K
fontdrvhost.exe	372	Console	1	11,988 K
fontdrvhost.exe	400	Services	0	6,600 K
svchost.exe	740	Services	0	10,316 K
svchost.exe	928	Services	0	45,552 K
svchost.exe	904	Services	0	23,908 K
svchost.exe	612	Services	0	12,676 K
dwm.exe	1100	Console	1	96,024 K
svchost.exe	1184	Services	0	13,088 K
svchost.exe	1824	Services	0	18,000 K
svchost.exe	1880	Services	0	16,824 K
svchost.exe	2000	Services	0	16,040 K
svchost.exe	1952	Services	0	28,048 K
svchost.exe	2032	Services	0	13,336 K
svchost.exe	1756	Services	0	15,596 K
NVDisplay.Container.exe	2092	Console	1	58,664 K
svchost.exe	2136	Services	0	17,552 K
svchost.exe	2168	Services	0	26,972 K
svchost.exe	2184	Services	0	16,752 K

svchost.exe	2192 Services	0	16,544 K
svchost.exe	2300 Services	0	21,336 K
svchost.exe	2340 Services	0	18,364 K
svchost.exe	2468 Services	0	28,164 K
svchost.exe	2548 Services	0	33,756 K
svchost.exe	2644 Services	0	19,756 K
svchost.exe	2652 Services	0	14,160 K
svchost.exe	2660 Services	0	16,404 K
svchost.exe	2736 Services	0	20,516 K
spoolsv.exe	2836 Services	0	39,808 K
svchost.exe	2920 Services	0	11,224 K
svchost.exe	2968 Services	0	6,936 K
svchost.exe	3040 Services	0	9,976 K
svchost.exe	2720 Services	0	12,996 K
dasHost.exe	3188 Services	0	9,276 K
svchost.exe	3464 Services	0	6,388 K
svchost.exe	3476 Services	0	7,380 K
SecurityHealthService.exe	3492 Services	0	10,356 K
chrome.exe	2908 Console	1	183,328 K
svchost.exe	6104 Services	0	6,840 K
chrome.exe	2112 Console	1	88,284 K
chrome.exe	972 Console	1	88,780 K
chrome.exe	10380 Console	1	42,104 K
LocationNotificationWindo	9892 Console	1	7,296 K
cmd.exe	5128 Console	1	3,184 K
conhost.exe	11600 Console	1	17,320 K
tasklist.exe	7984 Console	1	7,788 K
WmiPrvSE.exe	9084 Services	0	8,636 K

C:\Users\tsach>

IS-14 - October 24, 2017, 9:37 am

Its 30% and when i open task manager it goes back down to like 3%

5chn4pp - October 24, 2017, 10:51 am

Solution: keep your task manager running 24/7.

JK, do this scan:

Please download [Farbar Recovery Scan Tool](#) and save it to your Desktop.

Note: You need to run the version compatible with your system. If you are not sure which version applies to your system download both of them and try to run them. Only one of them will run on your system, that will be the right version.

Right click to run as administrator. When the tool opens click Yes to disclaimer.

Press Scan button.

It will produce logs called FRST.txt and Addition.txt in the same directory the tool is run from.

Please copy and paste the logs back here.

IS-14 - October 24, 2017, 12:42 pm

FRST https://mega.nz/#!zIdVnIrD!D7KFMIQ0aKvGw6v_6LwN_4M6NbKB9y3AoggBqBoWfW0
Addition https://mega.nz/#!ultyWDDR!j6zG0G1djecjPN4Jzsd37Elq8_-Q2uuKmQVx8EPiM2o
its a text doc , i couldnt upload the logs they were too long.

Zar66661 - October 24, 2017, 1:02 pm

You got a heavy load of the svchost services running, and it sounds like a silent miner. Best to check msconfig startup/services to see if "svchost.exe" is ticked to start on those tabs.

Zar66661 - October 24, 2017, 1:03 pm

Also pastebin is more hacx friendly my man.

Sparkfear - October 24, 2017, 1:10 pm

Seems sketchy.

Code AV: Windows Defender (Disabled - Up to date)
{D68DDC3A-831F-4fae-9E44-DA132C1ACF46}
AS: Windows Defender (Disabled - Up to date) {D68DDC3A-831F-4fae-9E44-DA132C1ACF46}
Code Imminent Monitor (HKLM-x32\...\Imminent Monitor) (Version: 5.0 - Imminent Methods)
CustomCLSID:
HKU\S-1-5-21-1947286723-1358728306-555116126-1001_Classes\CLSID\{4410DC33-BC7C-496B-AA84-4AEA3EEE75F7}\InprocServer32 ->
C:\Users\tsach\AppData\Local\Microsoft\OneDrive\17.3.7073.1013\amd64\FileCoAuthLib64.dll
(Microsoft Corporation)
Code 2017-10-23 01:22 - 2017-02-19 03:12 - 001240576 _____ ()
C:\Users\tsach\Desktop\PC\Imminent Methods\Imminent Monitor\bin\cef\CefSharp.Core.dll
2017-10-23 01:22 - 2017-02-19 03:12 - 066165760 _____ () C:\Users\tsach\Desktop\PC\Imminent
Methods\Imminent Monitor\bin\cef\libcef.dll
2017-10-23 01:22 - 2017-02-19 03:12 - 000822784 _____ () C:\Users\tsach\Desktop\PC\Imminent
Methods\Imminent Monitor\bin\cef\CefSharp.BrowserSubprocess.Core.dll
2017-10-23 01:22 - 2017-02-19 03:12 - 001886208 _____ () C:\Users\tsach\Desktop\PC\Imminent
Methods\Imminent Monitor\bin\cef\libglesv2.dll
2017-10-23 01:22 - 2017-02-19 03:12 - 000078848 _____ () C:\Users\tsach\Desktop\PC\Imminent
Methods\Imminent Monitor\bin\cef\libegl.dll
Meanwhile in your host
Code 127.0.0.1 jotti.org
127.0.0.1 viruschef.com
127.0.0.1 donotdistribute.com
127.0.0.1 www.jotti.org
127.0.0.1 www.viruschef.com
127.0.0.1 www.donotdistribute.com
127.0.0.1 www.metadefender.com
127.0.0.1 metadefender.com
Code FirewallRules: [TCP Query
User{2558B8E6-BC02-446D-A61B-D8A7F8C3B142}C:\users\tsach\desktop\dcrat\darkcomet.exe]
=> (Allow) C:\users\tsach\desktop\dcrat\darkcomet.exe
FirewallRules: [UDP Query
User{37AFCCCD-5402-4323-95BA-B34D5DCA0DF2}C:\users\tsach\desktop\dcrat\darkcomet.exe]
=> (Allow) C:\users\tsach\desktop\dcrat\darkcomet.exe
FirewallRules: [TCP Query
User{23378187-FFE1-421D-8E4B-52260A39B95A}C:\users\tsach\desktop\pc\hacking &
rats\dcrat\darkcomet.exe] => (Allow) C:\users\tsach\desktop\pc\hacking & rats\dcrat\darkcomet.exe

FirewallRules: [UDP Query
User{9F146AB6-BF86-49CA-ACA1-ED1A50D5A891}C:\users\tsach\desktop\pc\hacking &
rats\dcrat\darkcomet.exe] => (Allow) C:\users\tsach\desktop\pc\hacking & rats\dcrat\darkcomet.exe
Reason enough to believe you're infected..

IS-14 - October 24, 2017, 2:07 pm

reason enough not to, imminent monitor is my rat and the host is blocked by the coder of the crypter
i use...

GruntStyl - October 24, 2017, 2:24 pm

I know a lot of Miners will do such activity. I'm sure a lot of Spyware is starting to use the technique
now though as well.

IS-14 - October 24, 2017, 3:34 pm

guess no one here is smart enough to deal with this type of malware.

<https://imgur.com/a/JufCX> is svchost a virus? i have 5000 of those.

Linxy - October 24, 2017, 4:02 pm

<https://en.wikipedia.org/wiki/Svchost.exe>

It's built into Windows, but miners will name their applications "svchost.exe" to trick users into
thinking it is essential. It is normal for there to be more than one svchost.exe running on a windows
machine. Try a system recovery to a time that you did not see this happening, back track to any
applications you have ran that may have been questionable.

IS-14 - October 24, 2017, 4:17 pm

(Oct 24, 2017 04:02 PM)Linxy Wrote: [\[CITE\] https://en.wikipedia.org/wiki/Svchost.exe](https://en.wikipedia.org/wiki/Svchost.exe)

It's built into Windows, but miners will name their applications "svchost.exe" to trick users into
thinking it is essential. It is normal for there to be more than one svchost.exe running on a windows
machine. Try a system recovery to a time that you did not see this happening, back track to any
applications you have ran that may have been questionable.

why would any silent miner want only 30% of my cpu and not 90 ,100...

Kotlin - October 24, 2017, 4:40 pm

(Oct 24, 2017 04:17 PM)IS-14 Wrote: [\[CITE\]](#) why would any silent miner want only 30% of my cpu
and not 90 ,100...

I think you might've answered your own question there bud.

RumbleFrog - October 24, 2017, 4:41 pm

(Oct 24, 2017 04:17 PM)IS-14 Wrote: [\[CITE\]](#) why would any silent miner want only 30% of my cpu
and not 90 ,100...

Because it's way too noticeable at 90 or 100, it's called silent miner a reason.

Kotlin - October 24, 2017, 4:43 pm

(Oct 24, 2017 04:41 PM)RumbleFrog Wrote: [\[CITE\]](#) Because it's way too noticeable at 90 or 100, it's
called silent miner a reason.

Yeah, basically this OP. If it was at 90 or 100% usage at all time, the user can notice it fairly quick
and will probably fix it ASAP. However if it slowly mines, yeah it might take longer to make the same
amount as if it was at 100%; but the chance of the user noticing it will (presumably) take a lot longer
than usual.

5chn4pp - October 24, 2017, 11:29 pm

(Oct 24, 2017 01:10 PM)Sparkfear Wrote: [\[CITE\]](#) Seems sketchy.

Reason enough to believe you're infected..

None of those are malware indicators with the exception of the hosts file, nice try tho lol.

To OP:

Download [fixlist.txt](#) file and save it to the Desktop.

NOTE: It's important that both files, FRST/FRST64 and fixlist.txt are in the same location or the fix will not work.

NOTICE: This script was written specifically for this user, for use on that particular machine. Running this on another machine may cause damage to your operating system

Run FRST/FRST64 and press the Fix button just once and wait.

If for some reason the tool needs a restart, please make sure you let the system restart normally. After that let the tool complete its run.

When finished FRST will generate a log on the Desktop (Fixlog.txt). Please post it to your reply.

Hackswim - October 25, 2017, 12:22 pm

(Oct 24, 2017 10:51 AM)5chn4pp Wrote: [\[CITE\]](#) Solution: keep your task manager running 24/7.

JK, do this scan:

Please download [Farbar Recovery Scan Tool](#) and save it to your Desktop.

Note: You need to run the version compatible with your system. If you are not sure which version applies to your system download both of them and try to run them. Only one of them will run on your system, that will be the right version.

Right click to run as administrator. When the tool opens click Yes to disclaimer.

Press Scan button.

It will produce logs called FRST.txt and Addition.txt in the same directory the tool is run from.

Please copy and paste the logs back here.

made me laugh lol