

Forum:[Hack Forums](#)

Thread: [C: hidden files \(Program Files\)](#)

Pirate? - October 30, 2012, 12:14 pm

I just went into my hard drive and noticed that everything was missing, turned on hidden files and noticed

Games
PerfLogs
Program Files
Program Files (x86)
Program Data

were all hidden. I changed it back to normal with no problem, but I am wondering and worrying that it may be a problem it happened in the first place. Does anyone know how or what caused this to happen?

?Nano_Curie? - October 30, 2012, 12:22 pm

No idea , can you run scans with :

Malware bytes -
AVG (or whatever AV you have chosen) -
SpyBot search&destroy (or whatever anti-spyware you have chosen) -

Can you also post an image of your running processes and your startup programs
Via taskmanager/msconfig.

If you need assistance with any of the above feel free to PM me.

Pirate? - October 30, 2012, 1:57 pm

Processes: [\(Click to View\)](#)

Doing a MWB and Avast scan now, will update when they are finished.

?Nano_Curie? - October 30, 2012, 2:07 pm

Everything.exe , are you aware of the installation of any software in connection with
This process? If not please end it.

Pirate? - October 30, 2012, 2:52 pm

It's a program that shows like absolutely everything on my computer and is basically a better
windows search engine

http://download.cnet.com/Everything/3000-2379_4-10890746.html

EDIT: Scan Update (1 Hour)

MWB has found 2 objects so far (120,000 items scanned)

and Avast scan is at 10%

?Nano_Curie? - October 30, 2012, 3:18 pm

(Oct 30, 2012 02:52 PM)Pirate? Wrote: [CITE](#) It's a program that shows like absolutely everything on my computer and is basically a better windows search engine

http://download.cnet.com/Everything/3000-2379_4-10890746.html

EDIT: Scan Update (1 Hour)

MWB has found 2 objects so far (120,000 items scanned)

and Avast scan is at 10%

Awsome glad to see MWB has caught some, hopefully it can fix Without any fuss.

Pirate? - October 30, 2012, 4:15 pm

Results for Malwarebytes: [\(Click to View\)](#)

Malwarebytes Anti-Malware 1.65.1.1000

www.malwarebytes.org

Database version: v2012.10.30.08

Windows 7 x64 NTFS

Internet Explorer 9.0.8112.16421

Allan :: ALLAN-PC [administrator]

10/30/2012 4:57:11 PM

mbam-log-2012-10-30 (16-57-11).txt

Scan type: Full scan (C:\)

Scan options enabled: Memory | Startup | Registry | File System | Heuristics/Extra |

Heuristics/Shuriken | PUP | PUM

Scan options disabled: P2P

Objects scanned: 389247

Time elapsed: 2 hour(s), 16 minute(s), 10 second(s)

Memory Processes Detected: 0

(No malicious items detected)

Memory Modules Detected: 0

(No malicious items detected)

Registry Keys Detected: 0

(No malicious items detected)

Registry Values Detected: 0

(No malicious items detected)

Registry Data Items Detected: 0
(No malicious items detected)

Folders Detected: 0
(No malicious items detected)

Files Detected: 3
C:\Program Files (x86)\Square Enix\Sleeping Dogs\buddha.dll (Malware.Gen.SKR) -> No action taken.
C:\Windows\REMOVEWAT\REMOVEWAT.EXE (HackTool.Wpakill) -> No action taken.
C:\Users\Allan\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\830VPTE3\rkverify[1].exe (PUP.Adware.RelevantKnowledge) -> Quarantined and deleted successfully.

(end)

I'm not sure why it says Hacktool, but REMOVEWAT (Remove Windows Activation Technologies) removes the windows activation.

<http://www.mundu.org/?p=96>

More information: <http://answers.yahoo.com/question/index?qid=20100929190238AAng7vy>

So it's nothing to worry about, it's just considered dangerous by anti-virus.

And the buddha.dll is something used to get out of steam verification or something, a file I believe is from SKIDROW

?Nano_Curie? - October 30, 2012, 4:30 pm

I'm a little concerned you may have a RAT/Trojan on your system
Files don't just go hidden for no reason and with 3 malware detections
(false positives or not) it's a little fishy.

How's the avast scan coming along?

Also :

Spoiler ([Click to View](#)) HackTool.Wpakill is very dangerous and is not something that you want anywhere near your computer. HackTool.Wpakill is a deceptive software crack which is used by malicious people in order to avoid the Windows copy protection on the Microsoft Windows operating system. HackTool.Wpakill will try extremely hard to disable or bypass the Windows product activation code, by modifying your Windows operating system files, without your consent or knowledge.

source : <http://www.pcthreat.com/parasitebyid-8336en.html>

Did the Hacktool.wpaKill , get cured?
If not cure it immediately it may be what is messing with your files
Without your knowledge or permission.

Pirate? - October 30, 2012, 11:26 pm

(Oct 30, 2012 04:30 PM)2pros1cup Wrote: [\[CITE\]](#) I'm a little concerned you may have a RAT/Trojan on your system

Files don't just go hidden for no reason and with 3 malware detections (false positives or not) it's a little fishy.

How's the avast scan coming along?

Also :

Spoiler ([Click to View](#)) HackTool.Wpakill is very dangerous and is not something that you want anywhere near your computer. HackTool.Wpakill is a deceptive software crack which is used by malicious people in order to avoid the Windows copy protection on the Microsoft Windows operating system. HackTool.Wpakill will try extremely hard to disable or bypass the Windows product activation code, by modifying your Windows operating system files, without your consent or knowledge.

source : <http://www.pcthreat.com/parasitebyid-8336en.html>

Did the Hacktool.wpaKill , get cured?

If not cure it immediately it may be what is messing with your files

Without your knowledge or permission.

I already explained what the Hacktool.wpakill was from and that article says so even:

Quote:deceptive software crack which is used by malicious people in order to avoid the Windows copy protection on the Microsoft Windows operating system. HackTool.Wpakill will try extremely hard to disable or bypass the Windows product activation code

I am using a "not so genuine" copy of Windows 7 and this stops the activation process. That's all it is.

They say "very dangerous" because it is technically somewhat illegal and nobody likes that stuff. It's used for pirated windows copies.