

Forum:[Hack Forums](#)

Thread: [Malware-bytes deleted itself?](#)

Kayoz - March 20, 2014, 1:23 pm

So today I noticed something strange... I downloaded a trusted file (just stating that this can not be the source) and just for the lulz basically I was gonna virus-scan it with MalwareBytes. Then I noticed there was no "Scan with malware-bytes" button when I right clicked the file. Spoiler [\(Click to View\)](#) I then checked the "show hidden icon" thing down at the bottom right of the screen and I discovered that it wasn't even active. Spoiler [\(Click to View\)](#)

I then just searched "all programs" for it and I found it, but it had no icon image. Spoiler [\(Click to View\)](#)

Finally I tried to run the program and here is what the error message said...Spoiler [\(Click to View\)](#)

So now I basically want to know if this has happened to anybody else and/or if I should be worried and what I should do about it.

Thanks in advance!

Aura - March 20, 2014, 2:15 pm

This can sometimes be caused by a malware that have a feature to kill Malwarebytes and make it unusable to protect itself. Can you still launch it from it's folder in C:\Program Files (x86) ?

Kayoz - March 20, 2014, 2:19 pm

(Mar 20, 2014 02:15 PM)Aur? Wrote: [\[CITE\]](#) This can sometimes be caused by a malware that have a feature to kill Malwarebytes and make it unusable to protect itself. Can you still launch it from it's folder in C:\Program Files (x86) ?

Well I deleted the some things and now it's unusable anyways (not sure if it was unusable before) but when I try to delete the folder with malwarebytes, this is what comes up:

<http://prntscr.com/32loar>

Please help, I fucking hate being paranoid about everything.

EDIT: Also I have no fucking clue what this folder is, but it's protected aswell and seems shady.

<http://prntscr.com/32lpni>

Aura - March 20, 2014, 2:22 pm

(Mar 20, 2014 02:19 PM)Kayoz Wrote: [\[CITE\]](#) Well I deleted the some things and now it's unusable anyways (not sure if it was unusable before) but when I try to delete the folder with malwarebytes, this is what comes up: <http://prntscr.com/32loar>

Please help, I fucking hate being paranoid about everything.

Try to uninstall it instead of deleting the folder and reinstall it.

Kayoz - March 20, 2014, 2:26 pm

(Mar 20, 2014 02:22 PM)Aur? Wrote: [\[CITE\]](#) Try to uninstall it instead of deleting the folder and reinstall it.

Can't seem to find where to uninstall it, I've tried through CCleaner but I can't find the program there...

Should I just try to install it again without uninstalling and then doing a full virus scan?

Aura - March 20, 2014, 2:28 pm

(Mar 20, 2014 02:26 PM)Kayoz Wrote: [\[CITE\]](#) Can't seem to find where to uninstall it, I've tried through CCleaner but I can't find the program there...

Should I just try to install it again without uninstalling and then doing a full virus scan?

Yes try it and let me know if you can't install it. No need to do a full scan, do a quick scan, it's faster and as efficient as a full scan.

Kayoz - March 20, 2014, 2:30 pm

(Mar 20, 2014 02:28 PM)Aur? Wrote: [\[CITE\]](#) Yes try it and let me know if you can't install it. No need to do a full scan, do a quick scan, it's faster and as efficient as a full scan.

<http://prntscr.com/32lsxu>

That is what I got as error. Could [THIS](#) work?

Aura - March 20, 2014, 2:33 pm

(Mar 20, 2014 02:30 PM)Kayoz Wrote: [\[CITE\]](#) <http://prntscr.com/32lsxu>

That is what I got as error. Could [THIS](#) work?

Yes this is exactly the solution I was about to propose. Install the registry edit then take ownership of the Malwarebytes folder in ProgramData, delete it then click on "Retry".

Jagster™ - March 20, 2014, 2:34 pm

If you want to take ownership of a file/folder follow my guide [HERE](#)

Aura - March 20, 2014, 2:37 pm

(Mar 20, 2014 02:34 PM)Jagster Wrote: [\[CITE\]](#) If you want to take ownership of a file/folder follow my guide [HERE](#)

He's better of using the script Jagster. Sometimes this method doesn't even work on only the script is able to take ownership of the file/folder.

Jagster™ - March 20, 2014, 2:38 pm

(Mar 20, 2014 02:37 PM)Aur? Wrote: [\[CITE\]](#) He's better of using the script Jagster. Sometimes this method doesn't even work on only the script is able to take ownership of the file/folder.

Its included in there on the bottom :)

I feel like using the script is cheating haha ?

immortalwon - March 20, 2014, 2:38 pm

You might have plasma rat infection, use KFC cleaner

Kayoz - March 20, 2014, 2:51 pm

Well I had a bluescreen while trying to install malwarebytes but ill try again. Pretty sure avast interfered somehow. Also I noticed the boot time was fast as shit now compared to before so I got to be doing something right.

Edit: it bluescreened again.. Should I start in safe mode?

Aura - March 20, 2014, 2:52 pm

(Mar 20, 2014 02:51 PM)Kayoz Wrote: [\[CITE\]](#) Well I had a bluescreen while trying to install malwarebytes but ill try again. Pretty sure avast interfered somehow. Also I noticed the boot time

was fast as shit now compared to before so I got to be doing something right.

You might have disabled a few startup programs that were taking up all your resources. If you ever need help reinstalling or troubleshooting your system, send me a PM, I can assist you via Teamviewer.

Kayoz - March 20, 2014, 2:59 pm

(Mar 20, 2014 02:52 PM)Aur? Wrote: [\[CITE\]](#) You might have disabled a few startup programs that were taking up all your resources. If you ever need help reinstalling or troubleshooting your system, send me a PM, I can assist you via Teamviewer.

I'll download it but I have never used it before.

Aura - March 20, 2014, 3:01 pm

(Mar 20, 2014 02:59 PM)Kayoz Wrote: [\[CITE\]](#) I'll download it but I have never used it before.

You have the choice to install it or just execute it. In both cases, you just have to send the ID and the password to a person and he can connect to your computer remotely.

Kayoz - March 20, 2014, 3:03 pm

(Mar 20, 2014 03:01 PM)Aur? Wrote: [\[CITE\]](#) You have the choice to install it or just execute it. In both cases, you just have to send the ID and the password to a person and he can connect to your computer remotely.

What the fuck. I keep bluescreening from basically everything I do? Any tips? I know that I can start in safe mode but what do I do from there?

Aura - March 20, 2014, 3:07 pm

(Mar 20, 2014 03:03 PM)Kayoz Wrote: [\[CITE\]](#) What the fuck. I keep bluescreening from basically everything I do? Any tips? I know that I can start in safe mode but what do I do from there?

What did you delete exactly ? What changes did you made so far ?

Kayoz - March 20, 2014, 3:09 pm

(Mar 20, 2014 03:07 PM)Aur? Wrote: [\[CITE\]](#) What did you delete exactly ? What changes did you made so far ?

I deleted malwarebytes from appdata, programdata and program files along with a survey bypasser which seems fishy.

Aura - March 20, 2014, 3:11 pm

(Mar 20, 2014 03:09 PM)Kayoz Wrote: [\[CITE\]](#) I deleted malwarebytes from appdata, programdata and program files along with a survey bypasser which seems fishy.

You should have uninstalled instead of deleted the folders like that. Delete [BlueScreenView](#) and copy/paste the last BSOD entries on Pastebin and post the link here.

Kayoz - March 20, 2014, 3:18 pm

(Mar 20, 2014 03:11 PM)Aur? Wrote: [\[CITE\]](#) You should have uninstalled instead of deleted the folders like that. Delete [BlueScreenView](#) and copy/paste the last BSOD entries on Pastebin and post the link here.

I will try to just let my pc chill a couple mins to see if it bluescreens from some startup shit or if i'm triggering it manually somehow.

Confirmed, it is some startup shit that does the bluescreening as I didn't touch the computer and it still died.

Will try installing bluescreenview in safe mode now.

Currently installing Windbg to be able to open dmp files. Will update this when it's finished.

Aura - March 20, 2014, 3:33 pm

(Mar 20, 2014 03:18 PM)Kayoz Wrote: [\[CITE\]](#) I will try to just let my pc chill a couple mins to see if it bluescreens from some startup shit or if i'm triggering it manually somehow.

Confirmed, it is some startup shit that does the bluescreening as I didn't touch the computer and it still died.

Will try installing bluescreenview in safe mode now.

Currently installing Windbg to be able to open dmp files. Will update this when it's finished.

All good, keep us updated on the current situation.

Kayoz - March 20, 2014, 3:45 pm

(Mar 20, 2014 03:33 PM)Aur? Wrote: [\[CITE\]](#) All good, keep us updated on the current situation. Having big problems installing the windbg for some reason... Will try to find an alternative way to open dmp files.

Aura - March 20, 2014, 3:54 pm

(Mar 20, 2014 03:45 PM)Kayoz Wrote: [\[CITE\]](#) Having big problems installing the windbg for some reason... Will try to find an alternative way to open dmp files.

Look at my precedent post and use BlueScreenViewer.

Kayoz - March 20, 2014, 3:59 pm

(Mar 20, 2014 03:54 PM)Aur? Wrote: [\[CITE\]](#) Look at my precedent post and use BlueScreenViewer. I'm using BlueScreenViewer and it has saved my .dmp files, but I don't know how to open them.

edit: May have fixed it.

Edit2: The closest to sucess I've come is able to open it in a HTML and read it but it's a damn mess...

<http://pastebin.com/REfAimV1>

Aura - March 20, 2014, 4:00 pm

(Mar 20, 2014 03:59 PM)Kayoz Wrote: [\[CITE\]](#) I'm using BlueScreenViewer and it has saved my .dmp files, but I don't know how to open them.

You don't have to open them, it should open them as soon as you open BlueScreenViewer.

Kayoz - March 20, 2014, 4:06 pm

(Mar 20, 2014 04:00 PM)Aur? Wrote: [\[CITE\]](#) You don't have to open them, it should open them as soon as you open BlueScreenViewer.

I mean yeah it opens them but it's not anything I can copy and paste, I guess I could write the parts out that I can't paste.

Aura - March 20, 2014, 4:11 pm

(Mar 20, 2014 04:06 PM)Kayoz Wrote: [\[CITE\]](#) I mean yeah it opens them but it's not anything I can copy and paste, I guess I could write the parts out that I can't paste.

Of course you can copy and paste them. Or you can also take a screenshot of the BlueScreenView, upload it and post it there.

Kayoz - March 20, 2014, 4:50 pm

(Mar 20, 2014 04:11 PM)Aur? Wrote: [\[CITE\]](#) Of course you can copy and paste them. Or you can also take a screenshot of the BlueScreenView, upload it and post it there.

Pmed you a link with the bluescreenview report, hope this can get fixed as I'm not a big fan of using safe mode :L

Aura - March 20, 2014, 5:07 pm

(Mar 20, 2014 04:50 PM)Kayoz Wrote: [\[CITE\]](#) Pmed you a link with the bluescreenview report, hope this can get fixed as I'm not a big fan of using safe mode :L

This BSOD is caused by IO input on your HDD. Boot in Safe Mode, open an elevated command prompt and enter the follow command :

Code `chkdsk /r`

Plan the chkdsk for next reboot then reboot and let the chkdsk complete.

Kayoz - March 22, 2014, 5:39 am

(Mar 20, 2014 05:07 PM)Aur? Wrote: [\[CITE\]](#) This BSOD is caused by IO input on your HDD. Boot in Safe Mode, open an elevated command prompt and enter the follow command :

Code `chkdsk /r`

Plan the chkdsk for next reboot then reboot and let the chkdsk complete.

I still have a problem with this! I did the command and rebooted and let it complete fully which took a little less than 2 hours.

I didn't notice it doing anything at all and I still got bluescreen a minute after I started it in normal mode.

DpzFAsq4UEK8 - March 22, 2014, 6:42 am

You seem to be infected with Plasma RAT... My removal tool isn't complete yet.

Open cmd.exe as administrator and type this command then press enter:

Code `icacls C:\ProgramData /T /Q /C /RESET & icacls "C:\Program Files" /T /Q /C /RESET & icacls %APPDATA% /T /Q /C /RESET`It should make you able to delete the protected SecurityXploded directory and reinstall Malwarebytes.

Kayoz - March 22, 2014, 6:43 am

(Mar 22, 2014 06:42 AM)Arrhythmia Wrote: [\[CITE\]](#) You seem to be infected with Plasma RAT... My removal tool isn't complete yet.

Open cmd.exe as administrator and type this command then press enter:

Code `icacls C:\ProgramData /T /Q /C /RESET & icacls "C:\Program Files" /T /Q /C /RESET & icacls %APPDATA% /T /Q /C /RESET`

So what exactly does that command do? I'm worried about worsening my situation.

EDIT: didnt read entire post, I have already been able to "Delete" the malwarebytes although I cannot reinstall it. It bluescreens when I try to install even in safe mode.

DpzFAsq4UEK8 - March 22, 2014, 6:45 am

The command recursively resets permissions of ProgramData, Program Files, and AppData folders.

Anyways, I'd like to see a DDS log from you, sir.

Download [DDS](#) by SUBs to your desktop. Double click DDS.scr to run it and wait for the scan to finish

When finished DDS.txt and Attach.txt will open and be saved to your desktop.

Copy and paste the contents of both DDS.txt and Attach.txt into your next reply.

Kayoz - March 22, 2014, 6:59 am

(Mar 22, 2014 06:45 AM)Arrhythmia Wrote: [\[CITE\]](#) The command recursively resets permissions of ProgramData, Program Files, and AppData folders.

Anyways, I'd like to see a DDS log from you, sir.
Download [DDS](#) by SUBs to your desktop. Double click DDS.scr to run it and wait for the scan to finish

When finished DDS.txt and Attach.txt will open and be saved to your desktop.

Copy and paste the contents of both DDS.txt and Attach.txt into your next reply.

Ehm, there were like 650 lines of text on each one of them so I'll just post the pastebin link to both of them.

Also, I'm a little worried about what potential private info these may contain so I'll pm them to you instead. (example: "Post made by (my real name).")

DpzFAsq4UEK8 - March 22, 2014, 7:21 am

(Mar 22, 2014 06:59 AM)Kayoz Wrote: [\[CITE\]](#) Ehm, there were like 650 lines of text on each one of them so I'll just post the pastebin link to both of them.

Also, I'm a little worried about what potential private info these may contain so I'll pm them to you instead. (example: "Post made by (my real name).") I replied to your PM with an OTL fixlist. You have an obvious Plasma RAT infection.

Aura - March 22, 2014, 7:25 am

(Mar 22, 2014 07:21 AM)Arrhythmia Wrote: [\[CITE\]](#) I replied to your PM with an OTL fixlist. You have an obvious Plasma RAT infection.

Oh ? Is it time for [KFCCleaner](#) then ?!

DpzFAsq4UEK8 - March 22, 2014, 7:27 am

KFCleaner won't reset the permissions and IFEO's, I think. Correct me if I'm wrong.

Aura - March 22, 2014, 7:36 am

(Mar 22, 2014 07:27 AM)Arrhythmia Wrote: [\[CITE\]](#) KFCleaner won't reset the permissions and IFEO's, I think. Correct me if I'm wrong.

True. Well, IEFOs are easily deleted and I never encountered a permission issue with Plasma ?

DpzFAsq4UEK8 - March 22, 2014, 7:37 am

Plasma does set registry permissions on the IFEO's so they can't be deleted without restoring default permissions. It also sets the permission on itself, so the file cannot be deleted without using icacls to restore permission. And it also fucks up permissions of AV's files. At least it does that on my VM. Maybe it behaves differently on a real PC.

Kayoz - March 22, 2014, 12:01 pm

This has been completely and 100% solved by Arrhythmia and Aura. Thank you guys very much for sticking with me throughout this process :)

DpzFAsq4UEK8 - March 22, 2014, 12:02 pm

No problem.

Sorry for rendering your system unbootable, I don't know why this happened.

Aura - March 22, 2014, 4:33 pm

(Mar 22, 2014 07:37 AM)Arrhythmia Wrote: [\[CITE\]](#) Plasma does set registry permissions on the

IFEO's so they can't be deleted without restoring default permissions. It also sets the permission on itself, so the file cannot be deleted without using icacls to restore permission. And it also fucks up permissions of AV's files. At least it does that on my VM. Maybe it behaves differently on a real PC. Really ? Well, I always deleted the IFEOs via Autoruns and RogueKiller, so I never had this issue. It always worked. Just note that I execute both of them with Admin rights, that must be why. I couldn't tell to be honest, I would have to go delete the entries manually next time and see what it gives.

Also no problem OP, glad that your issue is solved ?

DpzFAsq4UEK8 - March 23, 2014, 12:31 am

Regedit ran with admin rights is unable to delete them. I always have to use subinacl or OTL to remove them.

Aura - March 23, 2014, 5:53 am

(Mar 23, 2014 12:31 AM)Arrhythmia Wrote: [\[CITE\]](#) Regedit ran with admin rights is unable to delete them. I always have to use subinacl or OTL to remove them.

Try Autoruns with Admin Rights. It looks like it gives itself permission or delete the entries a way regedit cant and it works.

DpzFAsq4UEK8 - March 23, 2014, 6:13 am

Well, I can also right click the registry key in regedit, then change the permissions from there.

Aura - March 23, 2014, 6:44 am

(Mar 23, 2014 06:13 AM)Arrhythmia Wrote: [\[CITE\]](#) Well, I can also right click the registry key in regedit, then change the permissions from there.

True. It's just a bit longer. The thing is that even if RogueKiller detect the IEFO entries and "deletes them", they're still present when I open Autoruns after RogueKiller. Maybe RogueKiller somehow requires a reboot in order for the entries to dissapear.

DpzFAsq4UEK8 - March 23, 2014, 6:45 am

That's probably because RogueKiller doesn't restore their permissions and just tries to remove them.

Aura - March 23, 2014, 6:47 am

(Mar 23, 2014 06:45 AM)Arrhythmia Wrote: [\[CITE\]](#) That's probably because RogueKiller doesn't restore their permissions and just tries to remove them.

Touché.

That's why Autoruns works I guess. Because it's a tool coming directly from Microsoft, it must have some permissions RogueKiller don't on these entries.