

Forum:[Hack Forums](#)

Thread: [Computer freezes on Bootup sometimes / sketchy Command Prompt](#)

I STOLE YOUR GF - May 11, 2016, 12:46 pm

Hey,
I don't know what is wrong with my system. Sometimes when I start it, it just freezes during the boot, and the power button cannot turn it off. (I have to open the case and unplug the battery, it's a laptop) Also sometimes while I'm just doing work or browsing my usual sites, YouTube or Facebook, a command prompt will quickly appear, show some lines of commands and then close itself before I can read what it is doing. I wish I had more information to give you but that's it. If anyone knows something I could do I would greatly appreciate it.
Thank you! ?

KrypteX - May 11, 2016, 4:29 pm

I'd have to take a better look to find out. I don't know how to use most of the tools that are commonly used in the whitehat section but if you'd like, I can definitely hop on skype and screenshare and I can either walk you through the process or I can offer you remote assistance, although most people find that sketchy.

I STOLE YOUR GF - May 11, 2016, 11:25 pm

Thanks, I know it probably won't happen, but I'd rather have someone who is official or trained for it help me with this. If I can't find help here there is a place in town I can go to, but I don't want to have to deal with people in person. Thanks though.

ProtectNull™ - May 12, 2016, 1:58 am

Hello I am here to assist you,

Please read these before we start with the procedures,
Please do not follow any other instructions other than mine, as they can cause conflict between my fixes.

Please be patient, as you can see I have other people to assist.

Please consider backing up any important files incase, (usually I will create System Restore Points if needed)

Please read the instructions carefully, as it can help a lot.

Do not login to valuable sites such as banking etc.

It is important that you do the instructions in order. (Up to Down)

[img]<http://nilights.info/wp-content/uploads/2014/05/divider.png>[img]

Before we do anything, I'll try to remove junks first.
Please download [Junkware Removal Tool](#) to your desktop.

Shut down your protection software now to avoid potential conflicts.

Run the tool by double-clicking it. If you are using Windows Vista, 7, or 8; instead of double-clicking, right-mouse click JRT.exe and select "Run as Administrator".

The tool will open and start scanning your system.

Please be patient as this can take a while to complete depending on your system's specifications.

On completion, a log (JRT.txt) is saved to your desktop and will automatically open.

Post the contents of JRT.txt into your next message.

[img]http://nilights.info/wp-content/uploads/2014/05/divider.png[/img]

Download this here [AdwCleaner](#)

Double click on AdwCleaner.exe to run the tool.

Click on the Scan button.

When it's done you'll see: Pending: Please uncheck elements you don't want removed.

Now click on the Report button...a logfile (AdwCleaner[R0].txt) will open in Notepad for review.

Look over the log especially under Files/Folders for any program you want to save.

If there's a program you may want to save, just uncheck it from AdwCleaner.

If you're not sure, post the log for review in pastebin.com and paste link in next reply.

If you're ready to clean it all up, click the Clean button.

After rebooting, a logfile report (AdwCleaner[S0].txt) will open automatically.

Copy and paste the contents of that logfile in your next reply.

A copy of that logfile will also be saved in the C:\AdwCleaner folder.

I STOLE YOUR GF - May 15, 2016, 12:40 am

~

Junkware Removal Tool (JRT) by Malwarebytes

Version: 8.0.6 (04.25.2016)

Operating System: Windows 10 Home x64

Ran by Matt (Administrator) on Sun 05/15/2016 at 3:24:44.10

~

File System: 8

Successfully deleted: C:\ProgramData\10866386157295603659 (Folder)

Successfully deleted: C:\ProgramData\summersoft (Folder)

Successfully deleted: C:\Users\Matt\AppData\Local\Google\Chrome\User Data\Default\Local Storage\chrome-extension_ogminpmlndcgcmmokldnmmmapddoccmhfl_0.localstorage (File)

Successfully deleted:

C:\Users\Matt\AppData\Roaming\Mozilla\Firefox\Profiles\ojcl5u12.default\extensions\bingsearch.full@microsoft.com\search.xml (File)

Successfully deleted:

C:\Users\Matt\AppData\Roaming\Mozilla\Firefox\Profiles\ojcl5u12.default\Invalidprefs.js (File)

Successfully deleted: C:\WINDOWS\system32\Tasks\PCEventLauncherTask (Task)

Successfully deleted: C:\WINDOWS\system32\Tasks\PCDoctorBackgroundMonitorTask (Task)

Successfully deleted: C:\Users\Matt\AppData\Roaming\appdataFr3.bin (File)

Registry: 2

Successfully deleted: HKCU\Software\Microsoft\Internet

Explorer\SearchScopes\{33BB0A4E-99AF-4226-BDF6-49120163DE86} (Registry Key)

Successfully deleted: HKCU\Software\Microsoft\Internet

Explorer\SearchScopes\{B301492C-4245-4078-9FC7-9F189D670FF1} (Registry Key)

~

Scan was completed on Sun 05/15/2016 at 3:26:39.76

End of JRT log

~

*** [Files] ***

*** [DLLs] ***

*** [WMI] ***

*** [Shortcuts] ***

*** [Scheduled tasks] ***

*** [Registry] ***

[-] Key Deleted : HKLM\SOFTWARE\Google\Chrome\NativeMessagingHosts\avgsh

[x] Key Not Deleted :

HKCU\Software\Google\Chrome\Extensions\lfcfenmboojpjjnhpgggodefccipikbpd

[-] Key Deleted : HKLM\SOFTWARE\Classes\ScriptHelper.GenericWnd

[-] Key Deleted : HKLM\SOFTWARE\Classes\ScriptHelper.GenericWnd.1

[-] Key Deleted : HKLM\SOFTWARE\Classes\ScriptHelper.NativeApi

[-] Key Deleted : HKLM\SOFTWARE\Classes\ScriptHelper.NativeApi.1

[-] Key Deleted : HKCU\Software\Classes\CLSID\{F28C2F70-47DE-4EA5-8F6D-7D1476CD1EF5}
[-] Key Deleted :
HKLM\SOFTWARE\Classes\CLSID\{B2BC04DF-EFBD-409A-95CA-36874E5AB92A}
[-] Key Deleted :
HKLM\SOFTWARE\Classes\CLSID\{CA3A5461-96B5-46DD-9341-5350D3C94615}
[-] Key Deleted : HKCU\Software\Classes\TypeLib\{157B1AA6-3E5C-404A-9118-C1D91F537040}
[x] Key Not Deleted :
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\PreApproved\{B2BC04DF-EFBD-409A-95CA-36874E5AB92A}
[x] Value Not Deleted : HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Ext\CLSID
[{3593C8B9-8E18-4B4B-B7D3-CB8BEB1AA42C}]
[-] Key Deleted : HKCU\Software\WEBAPP
[-] Key Deleted :
HKU\DEFAULT\Software\AppDataLow\{12DA0E6F-5543-440C-BAA2-28BF01070AFA}
[-] Key Deleted :
HKU\S-1-5-21-2977089736-950357887-4028935304-1002\Software\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\windows_ie_ac_001\Software\Crossrider
[-] Key Deleted :
HKU\S-1-5-21-2977089736-950357887-4028935304-1002\Software\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\windows_ie_ac_001\Software\The weDownload Manager
*** [Web browsers] ***

[x] [C:\Users\Matt\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences
[Extension] Not Deleted : fcfenmboojpjjnhpgggodefccipikbpd

:: "Tracing" keys deleted
:: Winsock settings cleared

C:\AdwCleaner\AdwCleaner[C1].txt - [2431 bytes] - [15/05/2016 03:33:45]
C:\AdwCleaner\AdwCleaner[S1].txt - [2540 bytes] - [15/05/2016 03:29:17]

EOF - C:\AdwCleaner\AdwCleaner[C1].txt - [2577 bytes]

ProtectNull™ - May 15, 2016, 1:59 am

(May 15, 2016 12:40 AM)I STOLE YOUR GF Wrote: [\[CITE\]](#) ~

Junkware Removal Tool (JRT) by Malwarebytes

Version: 8.0.6 (04.25.2016)

Operating System: Windows 10 Home x64

Ran by Matt (Administrator) on Sun 05/15/2016 at 3:24:44.10

~

File System: 8

Successfully deleted: C:\ProgramData\10866386157295603659 (Folder)

Successfully deleted: C:\ProgramData\summersoft (Folder)

Successfully deleted: C:\Users\Matt\AppData\Local\Google\Chrome\User Data\Default\Local

Storage\chrome-extension_ogminpmlndncgcmokldnmmapddoccmhfl_0.localstorage (File)
Successfully deleted:
C:\Users\Matt\AppData\Roaming\Mozilla\Firefox\Profiles\ojcl5u12.default\extensions\bingsearch.full
@microsoft.com\search.xml (File)
Successfully deleted:
C:\Users\Matt\AppData\Roaming\Mozilla\Firefox\Profiles\ojcl5u12.default\Invalidprefs.js (File)
Successfully deleted: C:\WINDOWS\system32\Tasks\PCDEventLauncherTask (Task)
Successfully deleted: C:\WINDOWS\system32\Tasks\PCDoctorBackgroundMonitorTask (Task)
Successfully deleted: C:\Users\Matt\AppData\Roaming\appdataFr3.bin (File)

Registry: 2

Successfully deleted: HKCU\Software\Microsoft\Internet
Explorer\SearchScopes\{33BB0A4E-99AF-4226-BDF6-49120163DE86} (Registry Key)
Successfully deleted: HKCU\Software\Microsoft\Internet
Explorer\SearchScopes\{B301492C-4245-4078-9FC7-9F189D670FF1} (Registry Key)

~

Scan was completed on Sun 05/15/2016 at 3:26:39.76
End of JRT log

~

*** [Files] ***

*** [DLLs] ***

*** [WMI] ***

*** [Shortcuts] ***

*** [Scheduled tasks] ***

*** [Registry] ***

[-] Key Deleted : HKLM\SOFTWARE\Google\Chrome\NativeMessagingHosts\avgsh
[x] Key Not Deleted :
HKCU\Software\Google\Chrome\Extensions\fcfenmboojpjinhpgggodefccipikbpd
[-] Key Deleted : HKLM\SOFTWARE\Classes\ScriptHelper.GenericWnd
[-] Key Deleted : HKLM\SOFTWARE\Classes\ScriptHelper.GenericWnd.1
[-] Key Deleted : HKLM\SOFTWARE\Classes\ScriptHelper.NativeApi
[-] Key Deleted : HKLM\SOFTWARE\Classes\ScriptHelper.NativeApi.1
[-] Key Deleted : HKCU\Software\Classes\CLSID\{F28C2F70-47DE-4EA5-8F6D-7D1476CD1EF5}
[-] Key Deleted :
HKLM\SOFTWARE\Classes\CLSID\{B2BC04DF-EFBD-409A-95CA-36874E5AB92A}
[-] Key Deleted :
HKLM\SOFTWARE\Classes\CLSID\{CA3A5461-96B5-46DD-9341-5350D3C94615}

[-] Key Deleted : HKCU\Software\Classes\TypeLib\{157B1AA6-3E5C-404A-9118-C1D91F537040}
[x] Key Not Deleted :
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\PreApproved\{B2BC04DF-EFBD-409A-95CA-36874E5AB92A}
[x] Value Not Deleted : HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Ext\CLSID
[{3593C8B9-8E18-4B4B-B7D3-CB8BEB1AA42C}]
[-] Key Deleted : HKCU\Software\WEBAPP
[-] Key Deleted :
HKU\DEFAULT\Software\AppDataLow\{12DA0E6F-5543-440C-BAA2-28BF01070AFA}
[-] Key Deleted :
HKU\S-1-5-21-2977089736-950357887-4028935304-1002\Software\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppDataContainer\Storage\windows_ie_ac_001\Software\Crossrider
[-] Key Deleted :
HKU\S-1-5-21-2977089736-950357887-4028935304-1002\Software\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppDataContainer\Storage\windows_ie_ac_001\Software\The weDownload Manager
*** [Web browsers] ***

[x] [C:\Users\Matt\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences
[Extension] Not Deleted : fcfenmboojpjjnhpgggodefccipikbpd

:: "Tracing" keys deleted
:: Winsock settings cleared

C:\AdwCleaner\AdwCleaner[C1].txt - [2431 bytes] - [15/05/2016 03:33:45]
C:\AdwCleaner\AdwCleaner[S1].txt - [2540 bytes] - [15/05/2016 03:29:17]

EOF - C:\AdwCleaner\AdwCleaner[C1].txt - [2577 bytes] #####Please
download [RougeKiller](#) and save the file to your Desktop.

Right-Click RougeKiller.exe and select Run as Administrator

Click Scan. Do not use the computer during the scan.

A log will be created and saved to the root directory. Paste the file contents to pastebin.com and post the link in your next reply.

I STOLE YOUR GF - May 15, 2016, 6:08 pm

RogueKiller V12.2.0.0 [May 10 2016] (Free) by Adlice Software

mail : <http://www.adlice.com/contact/>

Feedback : <http://forum.adlice.com>

Website : <http://www.adlice.com/software/roguekiller/>

Blog : <http://www.adlice.com>

Operating System : Windows 10 (10.0.10586) 64 bits version

Started in : Normal mode

User : Matt [Administrator]

Started from : C:\Users\Matt\Downloads\RogueKiller.exe
Mode : Scan -- Date : 05/15/2016 21:07:31

Processes : 0

Registry : 2

[PUM.SearchPage] (X64)

HKEY_USERS\S-1-5-21-2977089736-950357887-4028935304-1002\Software\Microsoft\Internet Explorer\Main | Search Bar : Preserve -> Found

[PUM.SearchPage] (X86)

HKEY_USERS\S-1-5-21-2977089736-950357887-4028935304-1002\Software\Microsoft\Internet Explorer\Main | Search Bar : Preserve -> Found

Tasks : 0

Files : 1

[File.Forged|VT.Unknown][File] C:\Windows\System32\drivers\hxxMVmor.sys -> Found

Hosts File : 0

Antirootkit : 0 (Driver: Not loaded [0xc000036b])

Web browsers : 0

MBR Check :

+++++ PhysicalDrive0: Hitachi HTS727575A9E364 +++++

--- User ---

[MBR] 2ce049b17bb975a7964002ffd869d691

[BSP] 55f171ca5eefd1b4137c12723b6e6095 : Empty|VT.Unknown MBR Code

Partition table:

0 - [MAN-MOUNT] EFI system partition | Offset (sectors): 2048 | Size: 500 MB

1 - [SYSTEM][MAN-MOUNT] Basic data partition | Offset (sectors): 1026048 | Size: 40 MB

2 - [MAN-MOUNT] Microsoft reserved partition | Offset (sectors): 1107968 | Size: 128 MB

3 - [SYSTEM][MAN-MOUNT] Basic data partition | Offset (sectors): 1370112 | Size: 490 MB

4 - Basic data partition | Offset (sectors): 2373632 | Size: 703269 MB

5 - [SYSTEM][MAN-MOUNT] | Offset (sectors): 1442670592 | Size: 820 MB

6 - [SYSTEM][MAN-MOUNT] | Offset (sectors): 1444349952 | Size: 350 MB

7 - [SYSTEM][MAN-MOUNT] Microsoft recovery partition | Offset (sectors): 1445066752 | Size: 9804 MB

User = LL1 ... OK

User = LL2 ... OK

=====

Thank you so much for helping me by the way

ProtectNull™ - May 15, 2016, 9:31 pm

(May 15, 2016 06:08 PM) STOLE YOUR GF Wrote: [\[CITE\]](#) RogueKiller V12.2.0.0 [May 10 2016] (Free) by Adlice Software

mail : <http://www.adlice.com/contact/>

Feedback : <http://forum.adlice.com>

Website : <http://www.adlice.com/software/roguekiller/>

Blog : <http://www.adlice.com>

Operating System : Windows 10 (10.0.10586) 64 bits version
Started in : Normal mode
User : Matt [Administrator]
Started from : C:\Users\Matt\Downloads\RogueKiller.exe
Mode : Scan -- Date : 05/15/2016 21:07:31

Processes : 0

Registry : 2

[PUM.SearchPage] (X64)

HKEY_USERS\S-1-5-21-2977089736-950357887-4028935304-1002\Software\Microsoft\Internet Explorer\Main | Search Bar : Preserve -> Found

[PUM.SearchPage] (X86)

HKEY_USERS\S-1-5-21-2977089736-950357887-4028935304-1002\Software\Microsoft\Internet Explorer\Main | Search Bar : Preserve -> Found

Tasks : 0

Files : 1

[File.Forged|VT.Unknown][File] C:\Windows\System32\drivers\hxxMVmor.sys -> Found

Hosts File : 0

Antirootkit : 0 (Driver: Not loaded [0xc000036b])

Web browsers : 0

MBR Check :

+++++ PhysicalDrive0: Hitachi HTS727575A9E364 +++++

--- User ---

[MBR] 2ce049b17bb975a7964002ffd869d691

[BSP] 55f171ca5eefd1b4137c12723b6e6095 : Empty|VT.Unknown MBR Code

Partition table:

0 - [MAN-MOUNT] EFI system partition | Offset (sectors): 2048 | Size: 500 MB

1 - [SYSTEM][MAN-MOUNT] Basic data partition | Offset (sectors): 1026048 | Size: 40 MB

2 - [MAN-MOUNT] Microsoft reserved partition | Offset (sectors): 1107968 | Size: 128 MB

3 - [SYSTEM][MAN-MOUNT] Basic data partition | Offset (sectors): 1370112 | Size: 490 MB

4 - Basic data partition | Offset (sectors): 2373632 | Size: 703269 MB

5 - [SYSTEM][MAN-MOUNT] | Offset (sectors): 1442670592 | Size: 820 MB

6 - [SYSTEM][MAN-MOUNT] | Offset (sectors): 1444349952 | Size: 350 MB

7 - [SYSTEM][MAN-MOUNT] Microsoft recovery partition | Offset (sectors): 1445066752 | Size: 9804 MB

User = LL1 ... OK

User = LL2 ... OK

=====

Thank you so much for helping me by the way

Download this here [ESET Online Scanner](#)

Turn off the real time scanner of any existing antivirus program while performing the online scan.

Tick the box next to YES, I accept the Terms of Use.

Click Start

Make sure that the option Remove found threats is unticked

Click on Advanced Settings and ensure these options are ticked

1) Scan for potentially unwanted applications

2) Scan for potentially unsafe applications

3) Enable Anti-Stealth Technology

Click Scan

Wait for the scan to finish

If any threats were found, click the 'List of found threats' , then click Export to text file....

Save it to your desktop, then please copy and paste that log to pastebin and paste the pastebin link to your next reply.

Please use pastebin.

I STOLE YOUR GF - May 16, 2016, 10:54 am

<http://pastebin.com/nnL7mj2i>

ProtectNull™ - May 16, 2016, 11:34 pm

(May 16, 2016 10:54 AM)I STOLE YOUR GF Wrote: [\[CITE\]](#) <http://pastebin.com/nnL7mj2i>

Download this here [RKILL](#)

Double-click on the Rkill icon to run the tool.

If using Vista or Windows 7/8/10, right-click on it and Run As Administrator.

A black DOS box will briefly flash and then disappear. This is normal and indicates the tool ran successfully.

A log pops up at the end of the run. This log file is located at C:\rkill.log. Please post this in your next reply (pastebin link)

If you do not see the black box flash on the screen delete the icon from the desktop and go back to the link for the download, select the next button and try to run the tool again, continue to repeat this process using the remaining buttons until the tool runs.

I STOLE YOUR GF - May 17, 2016, 9:27 am

<http://pastebin.com/C9TMHBcr>

ProtectNull™ - May 17, 2016, 8:59 pm

Does your PC freeze on bootup?

I STOLE YOUR GF - May 17, 2016, 10:59 pm

Only occasionally, for example if I shut it down to take it to a friend's house it will freeze on first boot, then after I force reset it a few times it will start up. Could it be a hardware malfunction?

ProtectNull™ - May 18, 2016, 1:56 am

(May 17, 2016 10:59 PM)I STOLE YOUR GF Wrote: [\[CITE\]](#) Only occasionally, for example if I shut it down to take it to a friend's house it will freeze on first boot, then after I force reset it a few times it will start up. Could it be a hardware malfunction?

System Operating System? have you recently upgraded to it?

How long have you had your PC for?

Specs?

I STOLE YOUR GF - May 18, 2016, 11:23 am

Windows 10, not recently upgraded

Had PC since Sept 2013

16gb ram (2 8Gb sticks)

i7 4700MQ CPU

Dual NVIDIA GTX 765M's

750 GB HDD

Motherboard: ??

ProtectNull™ - May 18, 2016, 10:20 pm

(May 18, 2016 11:23 AM)I STOLE YOUR GF Wrote: [\[CITE\]](#) Windows 10, not recently upgraded

Had PC since Sept 2013

16gb ram (2 8Gb sticks)

i7 4700MQ CPU

Dual NVIDIA GTX 765M's

750 GB HDD

Motherboard: ??

Try

Go to Start Menu > click on Settings.

Type performance > choose Adjust the appearance and performance of Windows.

If the current setting is significantly less than the recommended, uncheck the Automatically manage paging file size for all drives box at the top of the same windows and then click on Custom size.

Enter the Recommended value in the Initial Size box, and a larger figure in the Maximum size box.

Click OK to save the new settings.

I STOLE YOUR GF - May 19, 2016, 3:10 am

Ok, I've just restarted my computer to allow the changes to take effect.

ProtectNull™ - May 19, 2016, 10:21 pm

(May 19, 2016 03:10 AM)I STOLE YOUR GF Wrote: [\[CITE\]](#) Ok, I've just restarted my computer to allow the changes to take effect.

Whats the result?

I STOLE YOUR GF - May 20, 2016, 6:22 pm

Hasn't been freezing anymore, I guess that fixed it.

ProtectNull™ - May 20, 2016, 10:18 pm

(May 20, 2016 06:22 PM)I STOLE YOUR GF Wrote: [\[CITE\]](#) Hasn't been freezing anymore, I guess that fixed it.

I declare you clean, please open another thread if you think you are infected again or have any symptoms of being infected.

You can remove all files and programs that I have used such and logs to avoid space consumption and conflict.

If you have any concerns please state them in your next reply. Otherwise your welcome ?

Please download [Delfix](#)

This tool will remove most of the tools I used to disinfect your system. Please delete any leftover logs, files, folders and tools which was not removed by DelFix can be deleted manually. Please download the Delfix File and Save it into your Desktop Directory

Right Click on Delfix and Run As Administrator.

Please check the following items

Activate UAC

Remove disinfection tools

Create Registry Backup

Purge System Restore

Reset System Settings

And then just click 'Run'

I STOLE YOUR GF - May 21, 2016, 6:30 am

Thank you very much! You guys are so helpful!