

Forum:[Hack Forums](#)

Thread: [My Antivirus found extension viruses on Google Chrome, but it can't remove it?](#)

FoxyBaconator - March 27, 2015, 4:41 pm

My antivirus found Managera and Extutil, but when I tried to remove them with the antivirus, it wouldn't remove them. Are these dangerous and should I be worried? And can anyone help? Thanks for any help.

HoshHash - March 27, 2015, 4:44 pm

Step 1.

Download and Execute [MalwareBytes-AntiMalware](#). Complete the installaion and agree thier Terms of service/Use. Once you have finished the Malwarebytes installaion go ahead and open MalwareBytes-Antimalware (If not already running) Make sure that you updated Malwarebytes Database before you are running a Scan. Once you have updated the Database, go ahead and Do a Threat Scan and once the Scan is finish press the "Quarantine all" button.

(It will ask you if you want to do a Reboot, Press "Yes/Ok")

To get the logs do the following:

History > Application Logs

Open the scan log file.

Click Export.

Choose to Export to .txt.

And save it to your desktop.

Pictures MBAM.

Spoiler [\(Click to View\)](#)

Step 2.

Download [Junkware Removal Tool](#) by Thisisu, Save it to your desktop and Right Click on the tool, Open it as a Administrator with Admin rights. Once you have executed the tool with Administartors rights. A Command Prompt Window/Black Box will popup on your Screen. Accept thier Terms of Service/Usage of the tool and Press any Key Stroke/X to Start the Scan. Once the Scan and Cleaning process is finish, a Log file called JRT.txt should been saved to your desktop or will Popup

on the screen. Please Copy and paste the logs in here

Pictures JRT

Spoiler ([Click to View](#))

Step 3.

Download [Adwcleaner](#) and Save it to your desktop, Right click on the tool and open it as a Administrator with Admin rights. Complete the installation and Agree their Terms of Service/Usage of the Tool. The tool should popup on your screen. Press the "Scan" button to begin the Scan, Once the Scanning is finish, Press the "Clean" Button to begin the cleaning process. Once the cleaning is finish, It will ask you to do a Reboot, Press "Yes/Ok". After you done the Reboot, Please Copy and paste the logs in here.

The logs should be saved on your desktop or C:\AdwCleaner\AdwCleaner[R0].txt

Pictures AdwCleaner

Spoiler ([Click to View](#))

Step 4.

[Reset Your Web Browser To Its Default Settings.](#)

Step 5.

Logs i want to have: Malwarebyte's, JRT.txt, Adwcleaner.txt Post all the logs in here

FoxyBaconator - March 27, 2015, 5:02 pm

(Mar 27, 2015 04:44 PM)Farfar Wrote: ([CITE](#)) Step 1.

Download and Execute [MalwareBytes-AntiMalware](#). Complete the installation and agree their Terms of service/Use. Once you have finished the Malwarebytes installation go ahead and open MalwareBytes-Antimalware (If not already running) Make sure that you updated Malwarebytes Database before you are running a Scan. Once you have updated the Database, go ahead and Do a Threat Scan and once the Scan is finish press the "Quarantine all" button.

(It will ask you if you want to do a Reboot, Press "Yes/Ok")

To get the logs do the following:

History > Application Logs

Open the scan log file.

Click Export.

Choose to Export to .txt.

And save it to your desktop.

Pictures MBAM.

Spoiler ([Click to View](#))

Step 2.

Download [Junkware Removal Tool](#) by Thisisu, Save it to your desktop and Right Click on the tool, Open it as a Administrator with Admin rights. Once you have executed the tool with Administartors rights. A Command Prompt Window/Black Box will popup on your Screen. Accept thier Terms of Service/Usage of the tool and Press any Key Stroke/X to Start the Scan. Once the Scan and Cleaning process is finish, a Log file called JRT.txt should been saved to your desktop or will Popup on the screen. Please Copy and paste the logs in here

Pictures JRT

Spoiler ([Click to View](#))

Step 3.

Download [Adwcleaner](#) and Save it to your desktop, Right click on the tool and open it as a Administartor with Admin rights. Complete the installion and Agree thier Terms of Service/Usage of the Tool. The tool should popup on your screen. Press the "Scan" button to begin the Scan, Once the Scanning is finish, Press the "Clean" Button to begin the cleaning process. Once the cleaning is finish, It will ask you to do a Reboot, Press "Yes/Ok". After you done the Reboot, Please Copy and paste the logs in here.

The logs should be saved on your desktop or C:\AdwCleaner\AdwCleaner[R0].txt

Pictures AdwCleaner

Spoiler ([Click to View](#))

Step 4.

[Reset Your Web Browser To Its Default Settings.](#)

Step 5.

Logs i want to have: Malwarebyte's, JRT.txt, Adwcleaner.txt Post all the logs in here

Ok currently doing this. Quick question, should I just copy and paste the logs into a post and just post it in this thread?

HoshHash - March 27, 2015, 5:06 pm

(Mar 27, 2015 05:02 PM)ekaJ Wrote: [\[CITE\]](#) Ok currently doing this. Quick question, should I just copy and paste the logs into a post and just post it in this thread? If the logs are too big, Paste them separated. If not, you can just paste all the logs in 1 post.

-Farfar.

FoxyBaconator - March 27, 2015, 5:24 pm

(Mar 27, 2015 05:06 PM)Farfar Wrote: [\[CITE\]](#) If the logs are too big, Paste them separated. If not, you can just paste all the logs in 1 post.

-Farfar.

my JRT scan has been on "Checking Registry" for a while. Is this normal?

HoshHash - March 27, 2015, 5:38 pm

(Mar 27, 2015 05:24 PM)ekaJ Wrote: [\[CITE\]](#) my JRT scan has been on "Checking Registry" for a while. Is this normal? Give it 20 min more, If its still on "Checking Registry", Then jump to step 3.

FoxyBaconator - March 27, 2015, 5:48 pm

(Mar 27, 2015 05:06 PM)Farfar Wrote: [\[CITE\]](#) If the logs are too big, Paste them separated. If not, you can just paste all the logs in 1 post.

-Farfar.

AdwCleaner v4.113 - Logfile created 27/03/2015 at 20:39:26

Updated 22/03/2015 by Xplode

Database : 2015-03-27.1 [Server]

Operating system : Windows 8.1 (x64)

Username :

Running from : C:\Users\\Desktop\AdwCleaner.exe

Option : Cleaning

*** [Services] ***

*** [Files / Folders] ***

File Deleted : C:\Users\\AppData\Local\Google\Chrome\User Data\Default\Local Storage\hxxp_www.metrolyrics.com_0.localstorage-journal

*** [Scheduled tasks] ***

*** [Shortcuts] ***

*** [Registry] ***

Key Deleted : HKLM\SOFTWARE\AVG SafeGuard toolbar

Data Deleted : HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings
[ProxyOverride] - .local

**** [Web browsers] ***

-\\ Internet Explorer v11.0.9600.17416

-\\ Google Chrome v41.0.2272.101

AdwCleaner[R0].txt - [1024 bytes] - [27/03/2015 20:22:59]

AdwCleaner[S0].txt - [959 bytes] - [27/03/2015 20:39:26]

EOF - C:\AdwCleaner\AdwCleaner[S0].txt - [1017 bytes]

Junkware Removal Tool (JRT) by Thisisu

Version: 6.4.6 (03.22.2015:1)

OS: Windows 8.1 x64

Ran by on Fri 03/27/2015 at 20:07:46.27

~ Services

~ Registry Values

~ Registry Keys

~ Files

Successfully deleted: [File] "C:\WINDOWS\wininit.ini"

~ Folders

Successfully deleted: [Folder] "C:\WINDOWS\syswow64\ai_recyclebin"

~ Event Viewer Logs were cleared

Scan was completed on Fri 03/27/2015 at 20:38:45.91

End of JRT log

Scan Date: 3/27/2015

Scan Time: 7:48:28 PM

Logfile: malbytes.txt

Administrator: Yes

Version: 2.00.4.1028

Malware Database: v2015.03.27.10

Rootkit Database: v2015.03.26.01

License: Free

Malware Protection: Disabled

Malicious Website Protection: Disabled

Self-protection: Disabled

OS: Windows 8.1

CPU: x64

File System: NTFS

User:

Scan Type: Threat Scan

Result: Completed
Objects Scanned: 369259
Time Elapsed: 14 min, 21 sec

Memory: Enabled
Startup: Enabled
Filesystem: Enabled
Archives: Enabled
Rootkits: Disabled
Heuristics: Enabled
PUP: Enabled
PUM: Enabled

Processes: 0
(No malicious items detected)

Modules: 0
(No malicious items detected)

Registry Keys: 0
(No malicious items detected)

Registry Values: 0
(No malicious items detected)

Registry Data: 0
(No malicious items detected)

Folders: 0
(No malicious items detected)

Files: 2
Backdoor.Bot, C:\ProgramData\Nimoru\GizmoSE, Quarantined,
[1d690f3b31597eb87760b66e27dc06fa],
Backdoor.Bot, C:\ProgramData\Nimoru\LicenseSE, Quarantined,
[9cea2e1c5535e056c414d4506e9536ca],

Physical Sectors: 0
(No malicious items detected)

(end)

HoshHash - March 27, 2015, 5:59 pm

How did it go after resetting the browser web settings to its default settings?

Step 1.

Download [Roguekiller](#) by Tigzy and Save it to your desktop, Right click on the file and open it as a Administrator. Roguekiller will do its prescan once you have executed it (Its takes a couple of Minutes). Now when the prescan is finish and you accepted thier Terms of usage, press the "Scan" Button to begin the scan. Once the scan is finish press the "Report" Button, a Notepad with logs should popup, Please paste them in here and wait for further instructions from me.

-Farfar

FoxyBaconator - March 27, 2015, 6:58 pm

(Mar 27, 2015 05:59 PM)Farfar Wrote: [\[CITE\]](#) How did it go after reseting the browser web settings to its default settings?

Step 1.

Download [Roguekiller](#) by Tigzy and Save it to your desktop, Right click on the file and open it as a Administartor. Roguekiller will do its prescan once you have executed it (Its takes a couple of Minutes). Now when the prescan is finish and you accepted thier Terms of usage, press the "Scan" Button to begin the scan. Once the scan is finish press the "Report" Button, a Notepad with logs should popup, Please paste them in here and wait for further instructions from me.

-FarfarRogueKiller V10.5.7.0 [Mar 22 2015] 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 8.1 (6.3.9200) 64 bits version

Started in : Normal mode

User : [Administrator]

Started from : C:\Users\\Desktop\RogueKiller.exe

Mode : Scan -- Date : 03/27/2015 21:57:38

Processes : 0

Registry : 5

[Hidden.From.SCM] (X64)

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VBoxAswDrv (\\C:\Program Files\AVAST Software\Avast\ng\vbbox\VBBoxAswDrv.sys) -> Found

[PUM.DesktopIcons] (X64)

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons\NewStartPanel | {20D04FE0-3AEA-1069-A2D8-08002B30309D} : 1 -> Found

[PUM.DesktopIcons] (X64)

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons\NewStartPanel | {59031a47-3f72-44a7-89c5-5595fe6b30ee} : 1 -> Found

[PUM.DesktopIcons] (X86)

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons\NewStartPanel | {20D04FE0-3AEA-1069-A2D8-08002B30309D} : 1 -> Found

[PUM.DesktopIcons] (X86)

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons\NewStartPanel | {59031a47-3f72-44a7-89c5-5595fe6b30ee} : 1 -> Found

Tasks : 1

[Suspicious.Path] \\Microsoft OneDrive Auto Update

Task-S-1-5-21-2975596168-152625335-3012749906-1002 --

%localappdata%\Microsoft\OneDrive\OneDrive.exe -> Found

Files : 0

Hosts File : 0 [Too big!]

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

Web browsers : 0

MBR Check :

+++++ PhysicalDrive0: ST1000LM024 HN-M101MBB +++++

--- User ---

[MBR] a84dd93b5b19931ceaddbccc47850486

[BSP] df4f83c1f72e36823a12b0dfc7617313 : Empty MBR Code

Partition table:

0 - [MAN-MOUNT] EFI system partition | Offset (sectors): 2048 | Size: 300 MB

1 - [SYSTEM][MAN-MOUNT] Basic data partition | Offset (sectors): 616448 | Size: 900 MB

2 - [MAN-MOUNT] Microsoft reserved partition | Offset (sectors): 2459648 | Size: 128 MB

3 - Basic data partition | Offset (sectors): 2721792 | Size: 932050 MB

4 - [SYSTEM][MAN-MOUNT] Basic data partition | Offset (sectors): 1911560192 | Size: 20490 MB

User = LL1 ... OK

User = LL2 ... OK

HoshHash - March 29, 2015, 7:12 am

Since the problem is solved, Consider the thread as closed.