

Forum:[Hack Forums](#)

Thread: [Cannot get rid of Norton Utilities 16](#)

TYLER - April 9, 2018, 2:06 am

Hello,

Recently I downloaded and installed Adobe Shockwave Player for testing purposes which I made sure Norton installer was unchecked. However, that didn't matter apparently because now I am receiving constant popups from Norton Utilities 16 notifying me the installation of Norton Utilities 16 has failed and obviously wants me to download their intrusive software. I have tried multiple things to get rid of it, and for some reason it isn't gone.

What I've done:Uninstalled Adobe Shockwave Player.

Checked the registry to ensure there's nothing there regarding Norton or Symantec.

Removed all files/directories associated with Norton and Symantec.

Removed Norton/Symantec from the Windows Task Scheduler.

There's nothing in Add/Uninstall via Control Panel.

Ran Malwarebytes and Avast.

Ran the Norton Utilities Uninstaller from BleepingComputer.

Checked msconfig to ensure there's nothing under Services.

Checked Task Manger to ensure there's nothing under Startup.

Ran CCleaner to ensure there was nothing left behind.

Checked hidden files and folders.

Ran FRST and have logs if necessary. Just let me know and I will PM you the password.

Ran AdwCleaner and have logs if necessary. Just let me know and I will PM you with the password.

None of the above steps I've taken has successfully gotten rid of this crap. It's gotten to the point where when this popup appears, it re-adds the directories and files back to my system that I already deleted. It also creates a directory called "NortonWrapper" which disappears once I close the popup window.

I'm not sure what else to do. Any ideas?

Thanks!

Wires - April 9, 2018, 7:47 am

I'm Wires, I'm one of the students of the Security Malware Removal Team and will be assisting you throughout this thread. Before we start just take a second to read through these few requests - these are to ensure we can help you quickly and safely:Only use this thread for help. Please don't create multiple threads, accounts, PM me or post on other forums - if you do just let me know.

Only follow my guidance.

Don't run tools I haven't asked you to run. If you do just let me know so I can take that into consideration when viewing logs.

DO NOT install any other software while we are attempting to clean your machine. It can get quite confusing especially if you are downloading questionable tools.

Please be prompt in responding. I'll do my best to do so. If 48hrs has passed, please either PM me or ask "Are you there, I still need help" in this thread.

Please stick with me until I give you the 'All Clean'. I'll help you cleanup quickly and offer some tips

to make you more secure and get your system running faster.

Your malware related tools will be removed. I don't support the tools often distributed on these forums. Scanners will generally remove these - I take no responsibility for any malicious software that is lost.

I (nor does the forum) do not support pirated software.

If you don't understand something, don't be afraid to ask - I'm here to help. ?

You'll notice the logs are pretty big and you won't be able to post a reply containing it all. Please use ONLY either: <https://hastebin.com> - here you can upload the .txt file directly. - I prefer this. <http://pasted.co/> - here you can set a password if you wish to protect your data. Just PM me the password.

And paste the link to the logs in your reply. Post each log separately (each with a separate link). If you're a new member and can't paste links you can fool the forums system by removing the beginning of the link.

e.g. If you can't post this: <https://hastebin.com/raw/epaduvuyic>

Post: I used hastebin, here is the ending /raw/epaduvuyic

If I request you to post an image please use a service like <https://imgur.com>

=====

Did Malwarebytes and/or Avast detect anything at all on your system? If so, I'd like to see those logs if they're still available.

Malwarebytes - Log

Please post your log from Malwarebytes. Go into Malwarebytes executable, look for Reports in the side menu and select the log with the latest date. Copy and paste its content in your next reply.

Avast - Log

Please post your log from Avast. Go into Avast executable, look for Scan History in the bottom menu and select the log with the latest date. Copy and paste its content in your next reply.

As for Bleeping Computer's Norton Removal Tool, it does not include Norton Utilities 16.

Please post your AdwCleaner and FRST logs and then PM me the password if necessary.

=====

Please read the guide [AsSaSs@iN](https://hackforums.net/showthread.php?tid=5772641) constructed here before continuing:
<https://hackforums.net/showthread.php?tid=5772641>

Post the logs in THIS THREAD

How's the system running at this point?

TYLER - April 9, 2018, 6:00 pm

(Apr 9, 2018 07:47 AM)Wires Wrote: [\[CITE\]](#) -

Malwarebytes and Avast did not detect anything. I PM'd you the information for AdwCleaner and FRST.

Wires - April 10, 2018, 11:27 am

There isn't any Norton's product installed however it does seem there were some things left behind. We're going to go ahead and get rid of them.

Farbar Recovery Scan Tool (FRST) - Fix

Follow the instructions below to execute a fix on your system using FRST, and provide the log in your next reply. Open Notepad and copy/paste the following into notepad:

Code CloseProcesses:

CreateRestorePoint:

S2 RealtekWlanU; C:\Program Files (x86)\Realtek\USB Wireless LAN Utility\RtlService.exe [X]

S2 RunSwUSB; C:\Windows\runSW.exe [X]

S3 NPF; \SystemRoot\system32\DRIVERS\npf.sys [X]

S3 vmci; \SystemRoot\System32\drivers\vmci.sys [X]

S3 VMnetAdapter; \SystemRoot\system32\DRIVERS\vmnetadapter.sys [X]

2018-04-08 23:50 - 2018-04-08 23:50 - 000003324 _____ C:\Windows\System32\Tasks\Norton Product Installer

2018-04-08 23:50 - 2018-04-08 23:50 - 000000582 _____H C:\Windows\Tasks\Norton Product InstallerIdle.job

2018-04-08 23:50 - 2018-04-08 23:50 - 000000574 _____ C:\Windows\Tasks\Norton Product Installer.job

2018-04-06 16:43 - 2018-04-06 16:43 - 000000000 _____D

C:\Users\Tyler\AppData\Roaming\Product_NU16

2018-04-06 03:31 - 2018-04-08 23:50 - 000003218 _____ C:\Windows\System32\Tasks\Norton Product InstallerIdle

2018-03-30 21:07 - 2018-03-30 21:07 - 000000000 _____D C:\Users\Tyler\AppData\Roaming\NuGet

2018-03-30 18:19 - 2018-03-30 18:19 - 000000000 _____D C:\Program Files (x86)\NuGet

2018-04-08 21:04 - 2018-02-21 00:01 - 000002312 _____

C:\Windows\System32\Tasks\{A59DA323-B45F-4D23-B3CE-7D38AAB3E1AE}

2018-04-08 21:04 - 2018-02-20 23:56 - 000002312 _____

C:\Windows\System32\Tasks\{779A2F05-9121-4075-875C-75B8CFEAD533}

CustomCLSID:

HKU\S-1-5-21-1817824386-804169923-4099739089-1001_Classes\CLSID\{0E270DAA-1BE6-48F2-AC49-1AF02AB0DD12}\InprocServer32 -> %%%systemroot%%\system32\shell32.dll => No File

Task: {5812EE50-7695-42FF-8D98-0CAF9F551E52} -

System32\Tasks\{779A2F05-9121-4075-875C-75B8CFEAD533} => "c:\program files (x86)\google\chrome\application\chrome.exe"

hxxps://www.skype.com/go/downloading?source=lightinstaller&ver=7.40.0.104&LastError=404

Task: {5B7D883F-2EC4-4F4D-AB1F-499E1F2A1160} -

System32\Tasks\{A59DA323-B45F-4D23-B3CE-7D38AAB3E1AE} => "c:\program files (x86)\google\chrome\application\chrome.exe"

hxxps://www.skype.com/go/downloading?source=lightinstaller&ver=7.40.0.104&LastError=404

Task: {6F62F88A-654F-4473-BBF9-BE28057BCDE2} - System32\Tasks\Norton Product InstallerIdle => C:\Windows\SysWOW64\Macromed\Shockwave 10\SymInstallStub.exe

[2018-04-06] (Symantec Corporation)

Task: {9585BD96-A354-4A49-BF64-A1869FD003DF} - System32\Tasks\Norton Product Installer => C:\Windows\SysWOW64\Macromed\Shockwave 10\SymInstallStub.exe [2018-04-06] (Symantec Corporation)

Task: C:\Windows\Tasks\Norton Product Installer.job =>

C:\Windows\SysWOW64\Macromed\Shockwave 10\SymInstallStub.exe

Task: C:\Windows\Tasks\Norton Product InstallerIdle.job =>

C:\Windows\SysWOW64\Macromed\Shockwave 10\SymInstallStub.exe

EmptyTemp:

Save the file as fixlist.txt, and save it on your Desktop (or wherever your FRST.exe/FRST64.exe executable is located)

Right-click on the FRST executable and select Run as Administrator (for Windows Vista, 7, 8, 8.1 and 10 users)

Click on the Fix button

On completion, a message will come up saying that the fix has been completed and it'll open a log in Notepad

Copy and paste its content into your next reply

TYLER - April 11, 2018, 2:15 am

(Apr 10, 2018 11:27 AM)Wires Wrote: [CITE](#) There isn't any Norton's product installed however it does seem there were some things left behind. We're going to go ahead and get rid of them.

Farbar Recovery Scan Tool (FRST) - Fix

Follow the instructions below to execute a fix on your system using FRST, and provide the log in your next reply. Open Notepad and copy/paste the following into notepad:

```
CloseProcesses:CreateRestorePoint:S2 RealtekWlanU; C:\Program Files (x86)\Realtek\USB Wireless LAN Utility\RtlService.exe [X]S2 RunSwUSB; C:\Windows\runSW.exe [X]S3 NPF; \SystemRoot\system32\DRIVERS\npf.sys [X]S3 vmci; \SystemRoot\System32\drivers\vmci.sys [X]S3 VMnetAdapter; \SystemRoot\system32\DRIVERS\vmnetadapter.sys [X]2018-04-08 23:50 - 2018-04-08 23:50 - 000003324___ C:\Windows\System32\Tasks\Norton Product Installer2018-04-08 23:50 - 2018-04-08 23:50 - 000000582___H C:\Windows\Tasks\Norton Product InstallerIdle.job2018-04-08 23:50 - 2018-04-08 23:50 - 000000574___ C:\Windows\Tasks\Norton Product Installer.job2018-04-06 16:43 - 2018-04-06 16:43 - 000000000___D C:\Users\Tyler\AppData\Roaming\Product_NU162018-04-06 03:31 - 2018-04-08 23:50 - 000003218___ C:\Windows\System32\Tasks\Norton Product InstallerIdle2018-03-30 21:07 - 2018-03-30 21:07 - 000000000___D C:\Users\Tyler\AppData\Roaming\NuGet2018-03-30 18:19 - 2018-03-30 18:19 - 000000000___D C:\Program Files (x86)\NuGet2018-04-08 21:04 - 2018-02-21 00:01 - 000002312___ C:\Windows\System32\Tasks\{A59DA323-B45F-4D23-B3CE-7D38AAB3E1AE}2018-04-08 21:04 - 2018-02-20 23:56 - 000002312___ C:\Windows\System32\Tasks\{779A2F05-9121-4075-875C-75B8CFEAD533}CustomCLSID: HKU\S-1-5-21-1817824386-804169923-4099739089-1001_Classes\CLSID\{0E270DAA-1BE6-48F2-AC49-1AF02AB0DD12}\InprocServer32 -> %%systemroot%%\system32\shell32.dll => No FileTask: {5812EE50-7695-42FF-8D98-0CAF9F551E52} - System32\Tasks\{779A2F05-9121-4075-875C-75B8CFEAD533} => "c:\program files (x86)\google\chrome\application\chrome.exe" hxxps://www.skype.com/go/downloading?source=lightinstaller&ver=7.40.0.104&LastError=404Task: {5B7D883F-2EC4-4F4D-AB1F-499E1F2A1160} - System32\Tasks\{A59DA323-B45F-4D23-B3CE-7D38AAB3E1AE} => "c:\program files (x86)\google\chrome\application\chrome.exe" hxxps://www.skype.com/go/downloading?source=lightinstaller&ver=7.40.0.104&LastError=404Task: {6F62F88A-654F-4473-BBF9-BE28057BCDE2} - System32\Tasks\Norton Product InstallerIdle => C:\Windows\SysWOW64\Macromed\Shockwave 10\SymInstallStub.exe [2018-04-06] (Symantec Corporation)Task: {9585BD96-A354-4A49-BF64-A1869FD003DF} - System32\Tasks\Norton
```

Product Installer => C:\Windows\SysWOW64\Macromed\Shockwave 10\SymInstallStub.exe
[2018-04-06] (Symantec Corporation)Task: C:\Windows\Tasks\Norton Product Installer.job =>
C:\Windows\SysWOW64\Macromed\Shockwave 10\SymInstallStub.exeTask:
C:\Windows\Tasks\Norton Product InstallerIdle.job =>
C:\Windows\SysWOW64\Macromed\Shockwave 10\SymInstallStub.exeEmptyTemp: Save the file
as fixlist.txt, and save it on your Desktop (or wherever your FRST.exe/FRST64.exe executable is
located)

Right-click on the FRST executable and select Run as Administrator (for Windows Vista, 7, 8, 8.1
and 10 users)

Click on the Fix button

On completion, a message will come up saying that the fix has been completed and it'll open a log
in Notepad

Copy and paste its content into your next reply

Looks like my issue has been resolved. Thank you! ?