

# How to remove sality virus

## K. Sality Description

What is Sality?

This is a quote from [Norman website](#) :

“A family of fileinfecting viruses with backdoor and keylogger capabilities. Some variants install a helper component in the Windows System folder. Names on this component vary by Sality variant:

SYSLIB32.DLL (All early versions)  
OLEMDB32.DLL (Sality.M, version 3.03)  
WMIMGR32.DLL (Sality.N, version 3.04)  
VCMGRD32.DLL (Sality.P/Q, version 3.07)  
VCMGCD32.DLL (Sality.R, version 3.09)  
WDMFMC32.DLL (Sality.S, version 3.07)  
...and others.

This DLL is then injected into running processes.”

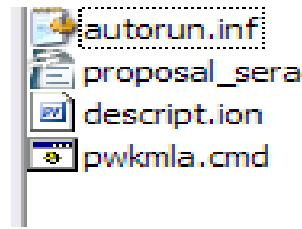
Another alias : Sality, Win32/Sality, Sality.AA, Sality.AE, Sality.AH, Sality.AM, Sality.AR

## L. How to know your computer is infected by Sality Virus :

These is the indications :

1. Task manager is disabled.
2. Registry Editor is disabled.
3. Show all hidden files and folders are not working .  
Hidden Files Folder setting always checks “Do not show hidden files and folder” option. You can't change the option, even if you check “Show hidden files and folder” option
4. Firewall and anti virus are not working.  
You can't run it and you can't scan with it; even you can run it and scan with it, the virus won't be found or the virus will be found but anti virus can't clean/delete it.
5. The virus infects .exe files on every partition of you harddisk.  
Almost all your .exe files on your computer will be infected (included explorer.exe, uninstall.exe, etc). Some of your .exe applications still may run, but some of them won't run (it will kill the runing process of infected .exe application or/and show an error message)!
6. The virus may infects some .com and .scr files.
7. The virus may infects some .dll files on your Windows folder.

8. If you plug in your USB Device on your computer, it will create an autorun.inf file + a random virus file.



**Pic1 :**

The virus created an autorun.inf file + a random virus file (pwkmla.cmd) on my sample UFD.

9. You can't boot your Windows in safe mode. You will failed if you try to boot your Windows in safe mode, and your system will restart automatically.

## M. Virus Removers

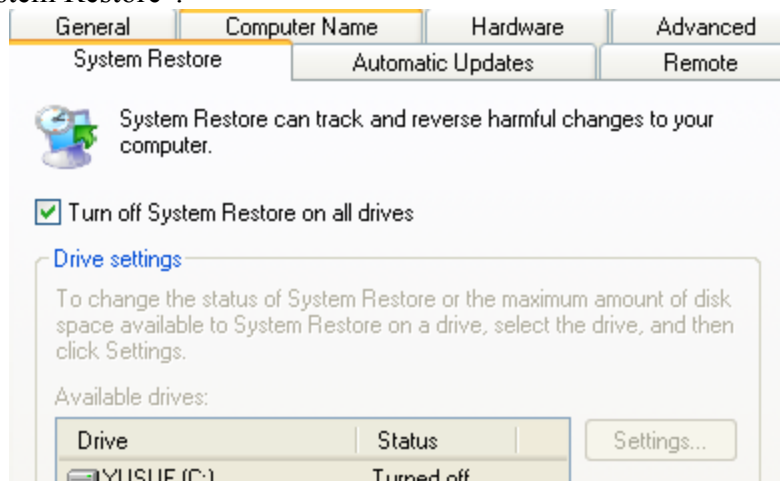
Before deleting the virus, you should download these tools :

1. Norman ~~Safiano~~ Malware Cleaner  
Choose one of these two links :  
Download 1 : [http://download.norman.no/public/Norman\\_Malware\\_Cleaner.exe](http://download.norman.no/public/Norman_Malware_Cleaner.exe)  
Download 2 : [http://normanasa.vo.llnwd.net/o29/public/Norman\\_Malware\\_Cleaner.exe](http://normanasa.vo.llnwd.net/o29/public/Norman_Malware_Cleaner.exe)
2. Symantec Win32.Sality.AE Removal Tool  
Choose one of these two links :  
Mirror Download 1 : <http://www.ziddu.com/download/3653712/FxSltyAE.rar.html>  
Mirror Download 2 : <http://rapidshare.com/files/233586434/FxSltyAE.rar.html>

## N. How to remove Sality Virus

How to remove sality virus :

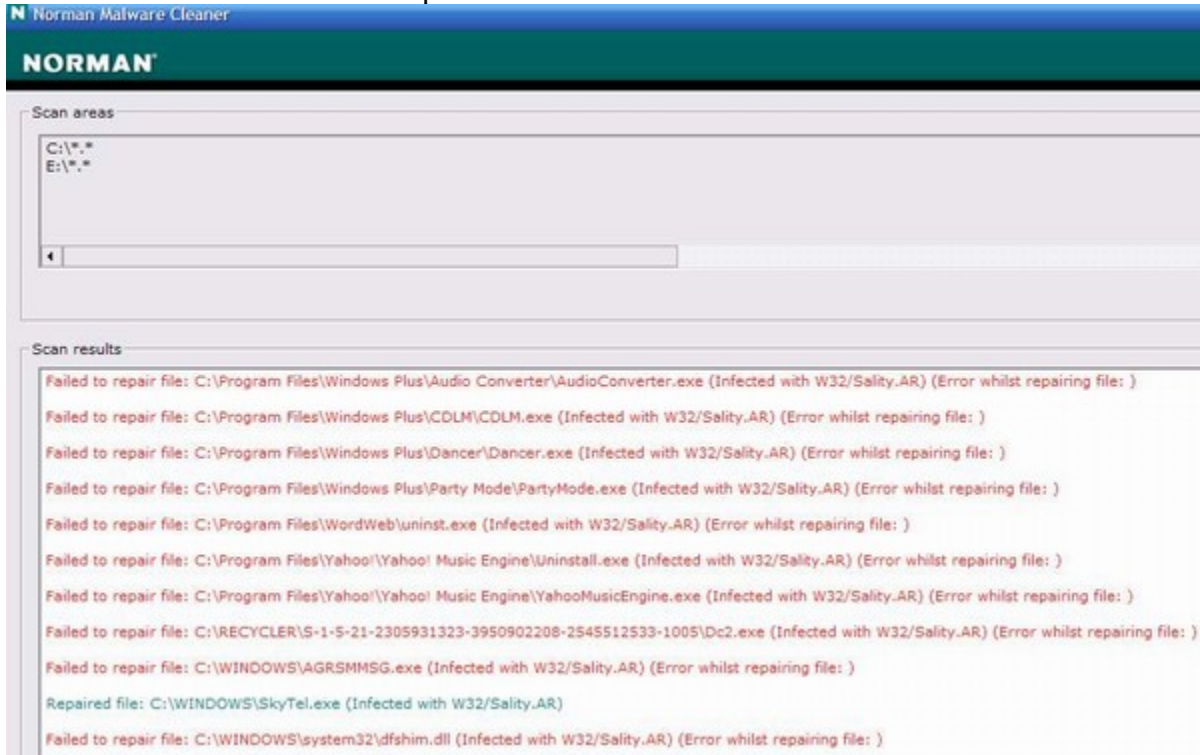
1. Turn off "System Restore".



**Pic2 :**

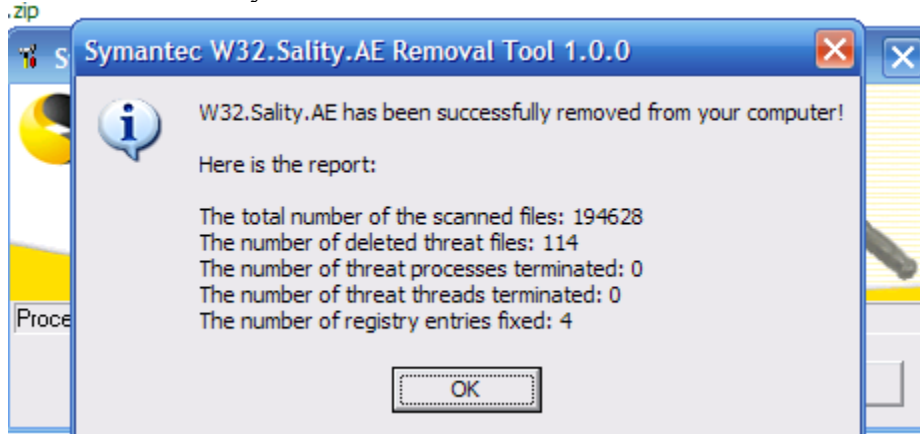
System restore

2. Run Norman Safiano what's up bro Malware Cleaner to scan the virus.



**Pic3 :**  
**Norman Malware Cleaner.**

3. If “do you want to restart...” dialog appears after scanning by Norman Safiano Malware Cleaner, you may restart or not restart.
4. If you want to restart, make sure the “System restore” is still turn off before restarting. After restarting, you should do step 1 to 2 again.
5. Run Symantec Win32.Sality.AE Removal Tool



**Pic4 :**  
**Symantec Win32.Sality.AE Removal Tool**

6. If “do you want to restart...” dialog appears after scanning by Symantec Win32.Sality.AE Removal Tool, you should restart. Make sure the “System restore” is still turn off before restarting.
7. After restarting, the virus most probably has been removed. Task manager and Registry Editor are re-enabled now.
8. To make sure the virus has been removed, run Symantec Win32.Sality.AE Removal Tool once again.

## O. Important Note

1. Sality virus most probably has been removed but maybe some files (exe, dll, etc) are still infected by Sality Virus. To clean it, you should scan it with your anti virus (NOD32, Kaspersky, Norman, Symantec, etc).
2. If anti virus can't clean it, you should delete the infected files (exe, dll, etc) BUT you should do it carefully and you should be more careful if the infected files exist on Windows Folder (example : explorer.exe etc). Before deleting, make sure the system will be fine if you delete it. If you're not sure, don't do it, or consult it to expert.
3. To repair safe mode, you can download the registry file to fix it :  
<http://www.eset.hk/support/tools/repairboot.zip>  
or  
[http://support.kaspersky.com/downloads/utills/sality\\_regkeys.zip](http://support.kaspersky.com/downloads/utills/sality_regkeys.zip)  
  
Extract, and run one file for your match system (safebootWinXP for windows XP, etc).
4. Re-installing Windows is not the best option, especially if your Windows license is not FPP/OLP. (Remember, if you re-install Windows, you must re-install driver & some softwares, etc and don't forget you should re-activate your Windows again). Re-formatting all of your hard disk partitions then re-installing Windows is the last option IF you want to do it.
5. I haven't re-formatted all of my hard disk partitions and re-installed Windows, because Sality virus has been removed and the infected files have been deleted carefully.

Yusuf KS (The S' abbreviation is not Sality!!)

p.s. If a problem's still occurred, you can ask it on comment, I'll help as best as I can.

Weblog : <http://myks.wordpress.com>

Permalink : <http://myks.wordpress.com/2009/05/16/how-to-remove-sality-virus/>

PDF Version : [http://www.kakikaku.com/yks/articles/how\\_to\\_remove\\_sality.pdf](http://www.kakikaku.com/yks/articles/how_to_remove_sality.pdf)