

Forum:[Hack Forums](#)

Thread: [Malware Bytes keeps popping up with the same malware](#)

Lynchings - June 23, 2015, 12:07 pm

Malware bytes keeps saying Malware Blocked and the file is C:/Windows/System32/ups10.dll

I did a full system scan with Malwarebytes and it says it removed this but it obviously didn't because it is still popping up. Can anybody please help me?

NoodleBot™ - June 23, 2015, 12:08 pm

Try booting into safe mode without networking and running the same scan again, the file is most likely being persistent.

Lynchings - June 23, 2015, 12:09 pm

(Jun 23, 2015 12:08 PM)NoodleBot™ Wrote: [\[CITE\]](#) Try booting into safe mode without networking and running the same scan again, the file is most likely being persistent. Would it be safe to just boot into safe mode and delete the file? I tried deleting it but it says I need permission from TrustedInstaller to remove it.

NoodleBot™ - June 23, 2015, 12:26 pm

Yes you may try that if are comfortable with removing it yourself rather than the scanning process again.

Ah trustedinstaller. Take ownership of the files (entire folder or files) with this script and delete again.

<https://hackforums.net/showthread.php?tid=3679336>

Tutorial | How to Take Ownership of a Folder and Files Inside

Kyle17 - June 23, 2015, 12:34 pm

My friend detected the exact same virus just 2 hours ago.

He got rid of it by using Junkware Removal Tool: <http://thisisudax.org/> (website with info)
<http://www.fosshub.com/Junkware-Removal-Tool.html> (Download page)

Just download,
Close all of the running programs if possible,
Wait for the scan to complete and do everything it says...

Good luck m8

Lynchings - June 23, 2015, 12:36 pm

(Jun 23, 2015 12:34 PM)Jacob Zuma Wrote: [\[CITE\]](#) My friend detected the exact same virus just 2 hours ago.

He got rid of it by using Junkware Removal Tool: <http://thisisudax.org/> (website with info)
<http://www.fosshub.com/Junkware-Removal-Tool.html> (Download page)

Just download,
Close all of the running programs if possible,
Wait for the scan to complete and do everything it says...

Good luck m8Thanks my man. Gonna do this now

EDIT: Didn't fix it at all. Trying to take ownership now with the script thing

Motiv - June 23, 2015, 4:26 pm

It could be set with persistence. Try going into msconfig and looking for anything suspicious. Be sure to google the program name before disabling something you don't know what it is.

READ: Please make sure that you delete that dumbass tool the guy with -9 rep just gave you.

Lynchings - June 23, 2015, 4:35 pm

Guys this was way worse than I thought. NoodleBot was teamviewing me and helping me remove this and he removed the infected DLL file which was apparently a system file. Doing so resulted in my entire Windows 7 install to be corrupted.

I've been going through hell and back to get it working, and I'm on a Live CD of Linux Mint right now. I need the proper version of USP10.dll for Windows 7 64 bit to fix this

Niko - June 23, 2015, 4:40 pm

(Jun 23, 2015 04:35 PM)Lynchings Wrote: [\[CITE\]](#) Guys this was way worse than I thought. NoodleBot was teamviewing me and helping me remove this and he removed the infected DLL file which was apparently a system file. Doing so resulted in my entire Windows 7 install to be corrupted.

I've been going through hell and back to get it working, and I'm on a Live CD of Linux Mint right now. I need the proper version of USP10.dll for Windows 7 64 bit to fix this

Theres a reason why you should always listen to one of the professionals, lately they have been quite busy, I am sorry that this had to happen.

Lynchings - June 23, 2015, 4:44 pm

(Jun 23, 2015 04:40 PM)LegitBytes Wrote: [\[CITE\]](#) Theres a reason why you should always listen to one of the professionals, lately they have been quite busy, I am sorry that this had to happen.I got my Windows 7 running right now, but it's still infected because I had to drag and drop the infected file right back into my System32 :/

Niko - June 23, 2015, 4:54 pm

After you do the following, ONLY take instructions from Knaut, Charmz and NullByte.

Please download Farbar Recovery Scan Tool. Make sure to get the one compatible with your system. <http://www.bleepingcomputer.com/download/farbar-recovery-scan-tool/>

Save it to your desktop.

Right click "Run as administrator"

Click Scan

It will output 2 logs "FRST.txt" and "Addition.txt" to your desktop. Post them on pastebin and reply with the links. Someone more advanced with malware removal will assist you in the removal process.

Lynchings - June 23, 2015, 5:01 pm

Addition.txt: <http://pastebin.com/xKB23JzW>

FRST.txt: <http://pastebin.com/zy97EJ8s>