How to remove OSDSoft Trojan DBUpdater.exe Miner

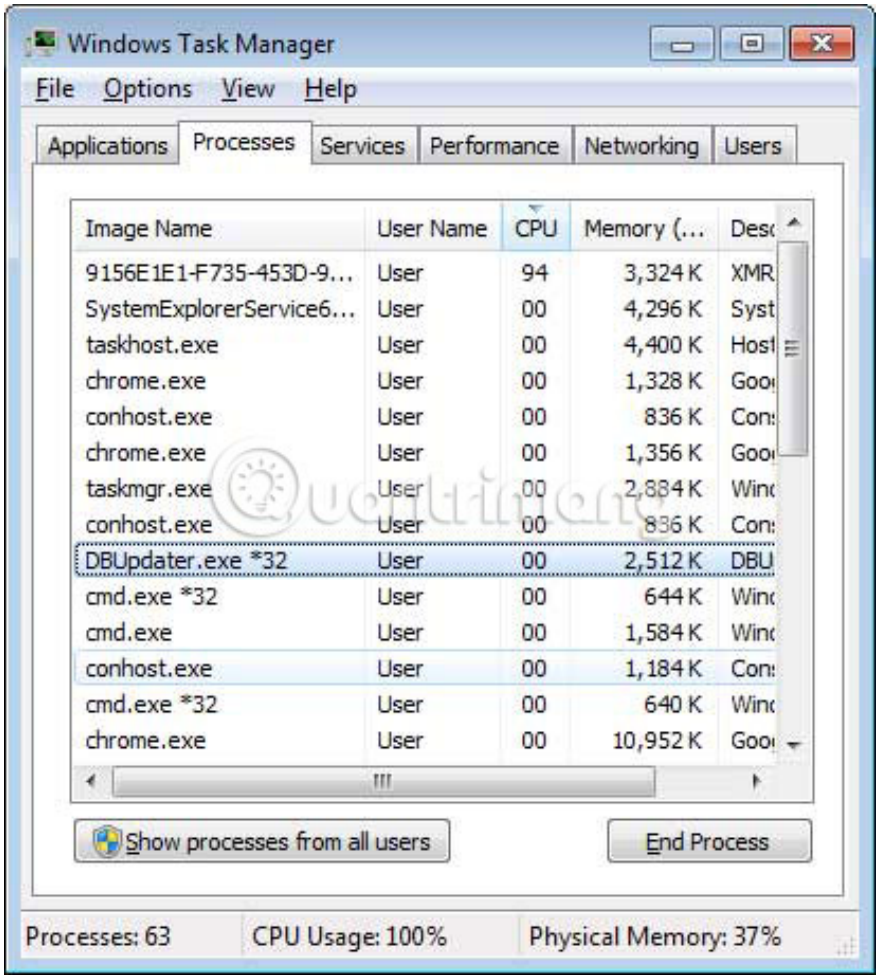
OSDSoft DBUpdater.exe Miner is a trojan that uses computer CPU resources to dig electronic money. When installed, the trojan launches an executable file with a random name, which uses up to 90% of the computer's CPU, when displayed in Task Manager.

OSDSoft DBUpdater.exe Miner is a trojan that uses computer CPU resources to dig electronic money. When installed, the trojan launches an executable file with a random name, which uses up to 90% of the computer's CPU, when displayed in Task Manager.

You should install a good antivirus software on your computer to prevent the risk of infection with these dangerous trojans.

OSDSoft Trojan Removal Guide DBUpdater.exe Miner

Identification sign OSDSoft DBUpdater.exe Miner

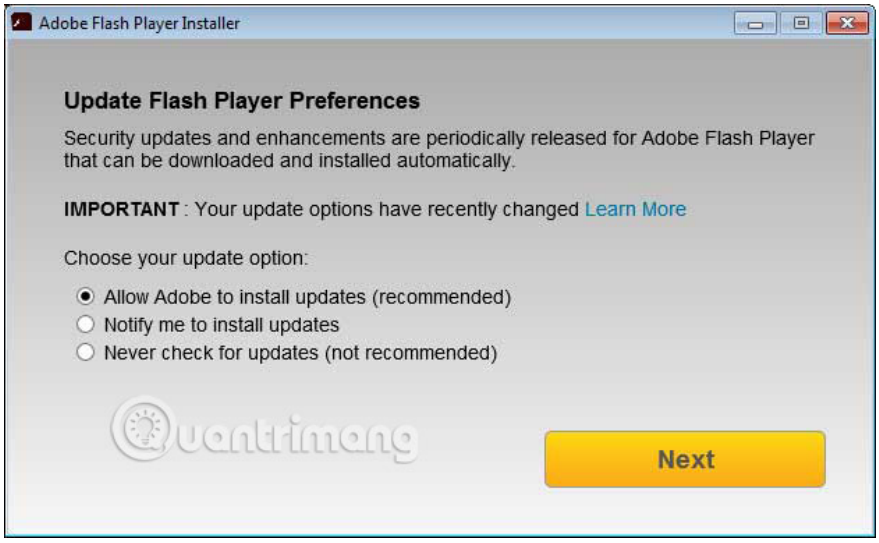


What is particularly worrisome about this type of trojan is that it will use the entire processing power of the CPU indefinitely, causing the CPU temperature to become very hot for a long time, gradually reducing the CPU's life. . There are no external signs for the user to know that the program is running, but to determine if the computer is infected with the trojan, check the following:

1. There is a process named randomly similar to 3246E2E2-D734-443D-343A-34EEC736EDA0.exe with the description XMRig uses almost 100% CPU.
2. Is there any process called DBUpdater.exe running in Task Manager.
3. Windows or games are slow and videos are jerky.
4. Are programs running slowly.
5. Task Manager shows that CPU usage is 100%.
6. The use of computers is slow (overall).

How is OSDSoft DBUpdater.exe Miner installed on the computer?

OSDSoft DBUpdater.exe Miner is installed by ad packages on the victim's computer without permission. You always remember to read all the information that appears when installing the software, make sure strange adware is not installed. In this example, the ad package is forging an Adobe Flash Player update.



This exploit tool consumes a lot of computer CPU resources. To protect the hardware and make the device work properly again, follow the instructions below to remove it.

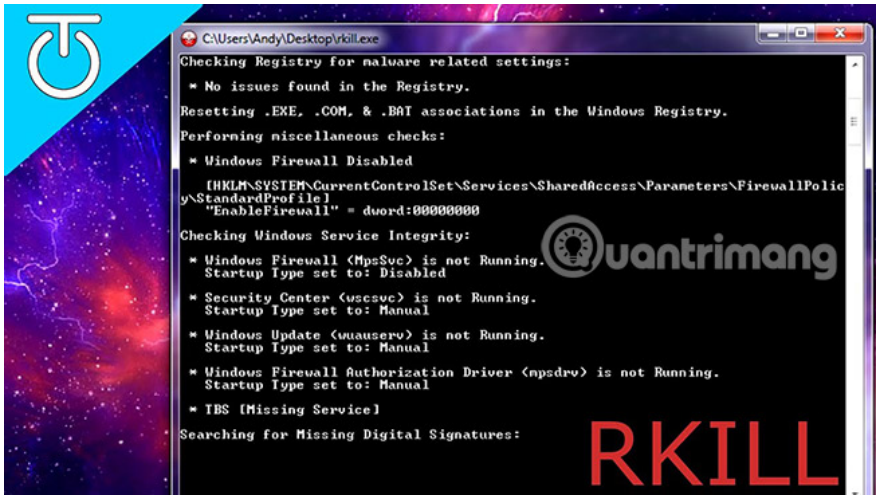
Options OSDSoft trojan removal DBUpdater.exe Miner

Note: Please back up the data before continuing.

To remove OSDSoft DBUpdater.exe Miner trojan, follow these steps:

1. Before using this tutorial, read through it once and download all the necessary tools to your computer first. Then, print the paper instructions because you may have to close the browser window or restart the computer.

2. To terminate any program, it may interfere with the process of removing trojans, first download the Rkill program. It will scan your computer for active malware and try to stop them so they don't interfere with the trojan removal process.



When on the download page, click the **Download Now** button **.** Then choose to save the file on the desktop.

3. After downloading, double-click the iExplore.exe icon to automatically stop any process related to OSDSoft DBUpdater.exe Miner trojan and other malware. Please wait patiently for the program to search for malware and end them. When finished, the black window will automatically close and a log file will open. Review the log file and then close it to continue with the next step. If you have trouble running RKill, you can download other RKill versions on the download page. Note that the download page will open in a new browser window or tab. Do not restart the computer after running RKill because malware programs will start running again.

4. Next, download Malwarebytes Anti-Malware, Zemana AntiMalware, AdwCleaner and HitmanPro software to scan the entire system. For details on how to do this, please refer to the article: Removing root malware (malware) on Windows 10 computers.

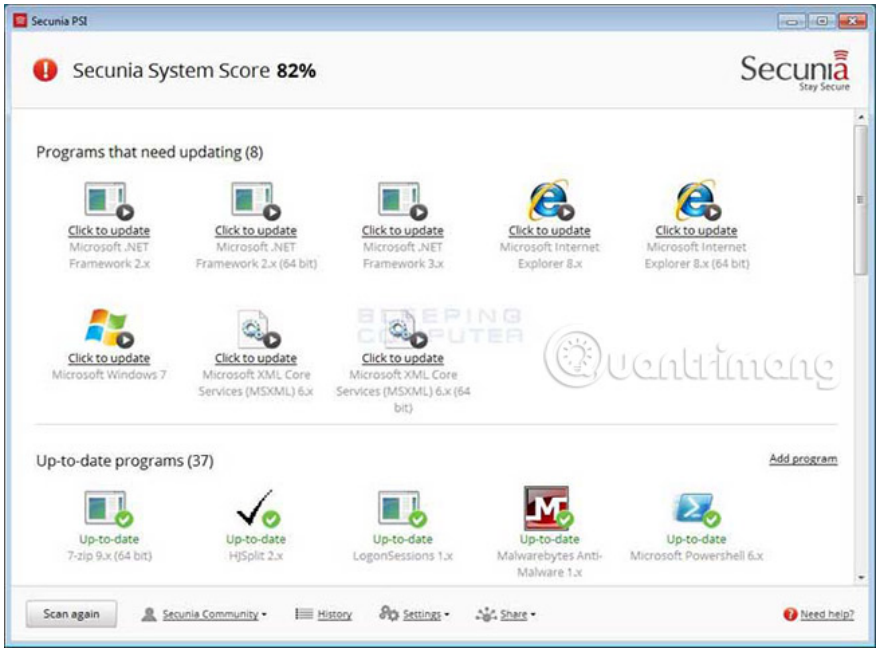
5. Since many malicious software and unwanted programs are installed through vulnerabilities found in outdated and unsafe programs, Secunia PSI should be used to scan easy programs. hacked on the computer.

To install Secunia Personal Software Inspector or Secunia PSI, first download the program here and save it to the desktop. After downloading, double-click the Secunia PSI icon

, Secunia PSI installer will start. Please follow the prompts to install the program. Leave a checkmark to install the automatic updates and click the **Next** button **.**

When the installation program is finished, you will be prompted if you want to launch Secunia PSI. Click the **Yes** button to allow the program to launch. Next time, if you want to restart the program, look for the program icon in Windows' Start menu.

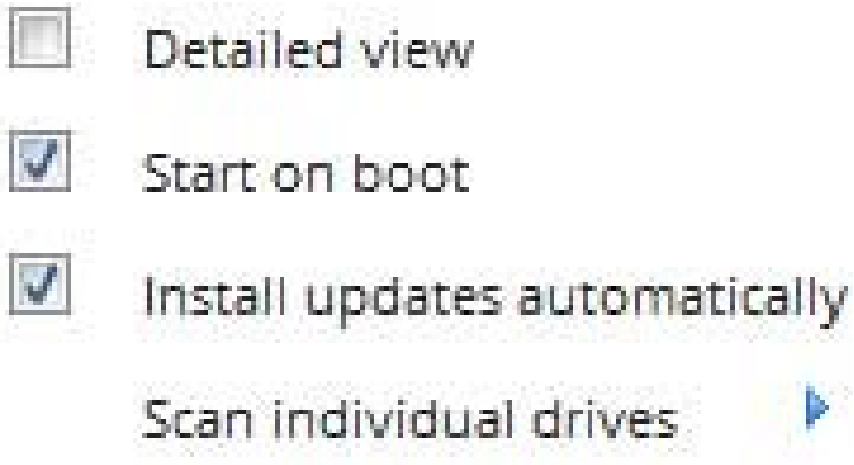
You will receive the message **Microsoft Update is not installed** and the prompt requires installation of the update. Microsoft Update is required to update Microsoft applications such as Office. If you do not see this message, then the update has been installed and you can move on to the next paragraph. If you receive a message, click the Install Microsoft Update button and allow it to open Internet Explorer. Internet Explorer will open on the Microsoft site where you will be able to download and install Microsoft Update. When on the Microsoft page, check the **I Agree** checkbox and then click **Next.** On the next page, select **Use recommended settings** and then click the **Install** button **.** Microsoft updates will be installed and when finished, you can close Internet Explorer and Windows Update, then return to the Secunia PSI screen. When returning to the Secunia PSI screen, click the **Close** button in the Microsoft Update message and you will be in the main screen of the program as shown below:



The screen above shows the list of programs installed on the computer and indicates whether they have been updated to the latest version. The top of the screen will also contain a number of points corresponding to the percentage of updated programs on the computer. Here, the computer has 37 updated programs and 8 programs to update. Secunia PSI can automatically update the program, without any help from users. However, if manual updates are required, click the **Click to update link** in each program icon and Secunia PSI will assist you to update or provide information on how to do so.

If you want to see more information about the program installed on your computer and why you need to update to the latest version, right-click on the program icon> select **More Information** , Secunia website will open in the browser and gives you more information about the program as well as security holes that exist in it.

To change whether updates, automatic settings or other configuration changes are made, click **Settings** at the bottom of the screen. A small menu like this will appear:



1. The **Start on boot** option specifies whether you want Secunia PSI to automatically start when you log into Windows and continue to run in the background. If the computer has a large memory, let this software run so that the computer is best protected.
2. The **Install updates** option **automatically** , you should choose to The program is updated automatically when new updates are available.
3. **Scan individual drives** option allows you to scan drives containing other applications and see if they need to be updated.
4. The last option is the **Detailed View** setting which displays the Secunia PSI status screen in more detail. Usually this option does not need to be activated.

You now know which programs are vulnerable to attacks on your computer. You should take a look at this list, download and install each update for the listed programs. In this way, you will eliminate any known vulnerabilities and protect your computer from the risk of remote hacking or installing malware on your computer without your permission.

When you have finished updating all programs, you can close the Secunia PSI program and it will continue to run in the background.

Your computer now has no**OSDSoft DBUpdater.exe Miner**trojan program.If the current security solution allows this program to be installed on your computer, you may want to consider purchasing the full-featured Malwarebytes Anti-Malware version to protect against these types of threats in the future. .

Good luck!

See more:

1. Learn about the Trojan.Win32.FraudPack.bkhe template
2. Find out about Virus.Win32.Sality.ag template
3. How to remove Baysearch.co

You finished reading the article "**How to remove OSDSoft Trojan DBUpdater.exe Miner**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.