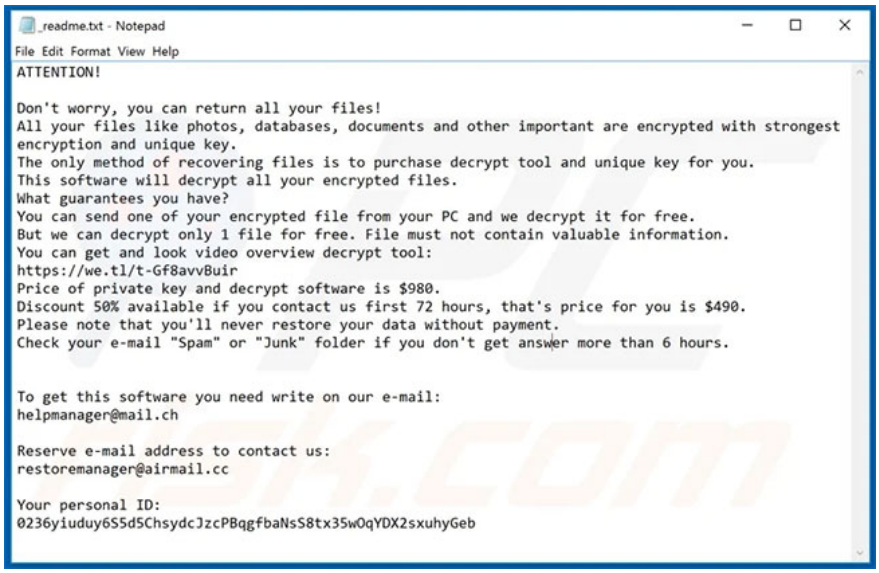
How to remove Moba ransomware from the operating system

Moba is a malware, belonging to the Djvu ransomware family. These malware-infected systems are encrypted data and receive a ransom request to obtain decryption tools / software.

Moba is a malware, belonging to the Djvu ransomware family. These malware-infected systems are encrypted data and receive a ransom request to obtain decryption tools / software.

During the encoding process, the files are added to the **".moba"** extension **.** After this process is completed, a ransom note - **"_readme.txt"** - will be placed into the compromised directory.



The ransom notes - "_readme.txt" - will be included in the compromised directories

remove Moba ransomware from the system

Step 1: Remove Moba virus with Safe Mode with Networking

1. For Windows XP and Windows 7 users: Start the computer in Safe Mode with one of two instructions:
    1. Start Safe Mode on Windows XP
    2. Enable Safe Mode in Windows 7
2. For Windows 8 users: Start Windows 8 in Safe Mode with Networking according to the instructions in the article: Windows 8: Start Safe Mode.

3. For Windows 10 users: Refer to the article: How to enter Safe Mode Windows 10 on startup for details on how to do it.

Step 2: Remove Moba ransomware with System Restore

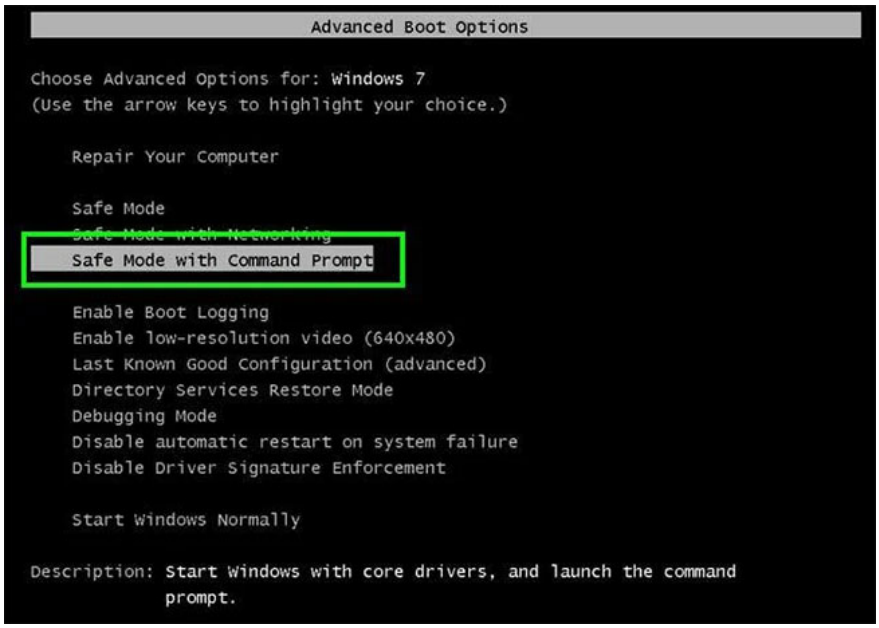
Login to Moba virus infected account. Start the Internet browser and download a legitimate anti-spyware program. Update the anti-spyware program and start scanning the entire system. Delete all detected items.

Download Malwarebytes
https://www.malwarebytes.com/pricing/

Malwarebytes will check to see if your computer is infected with malware. To use the full featured product, you must purchase a license for Malwarebytes after 14 days of free trial.

If you cannot boot your computer in Safe Mode with Networking, try performing System Restore.

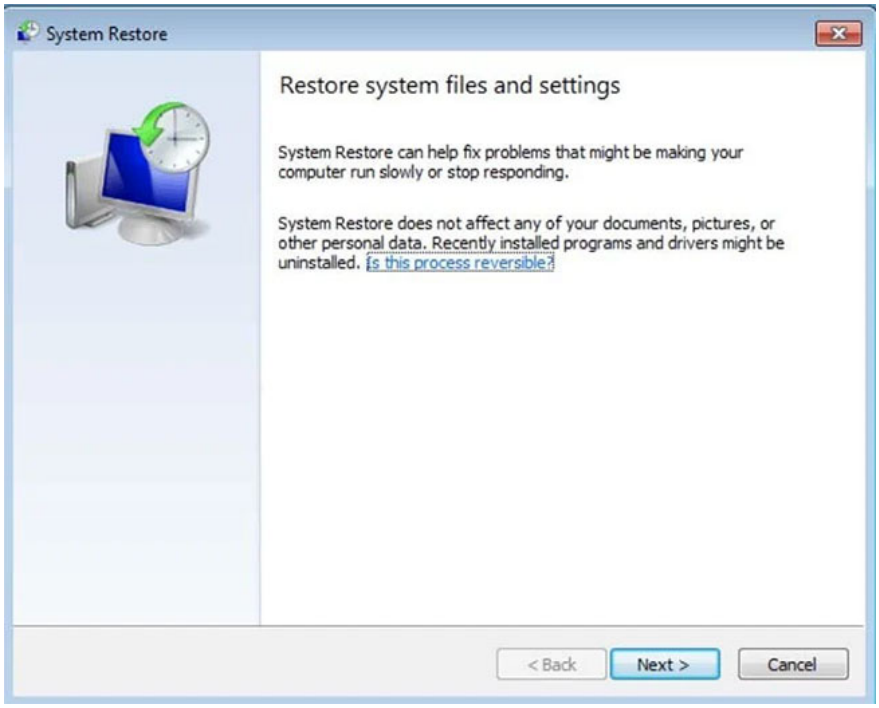
1. During booting the computer, press the key `F8`on the keyboard repeatedly until the **Windows Advanced Options** menu appears, then select **Safe Mode with Command Prompt** from the list and press `ENTER`.



Select Safe Mode with Command Prompt from the list
2. When **Command Prompt** mode loads, enter: `cd restore`and press `ENTER`.

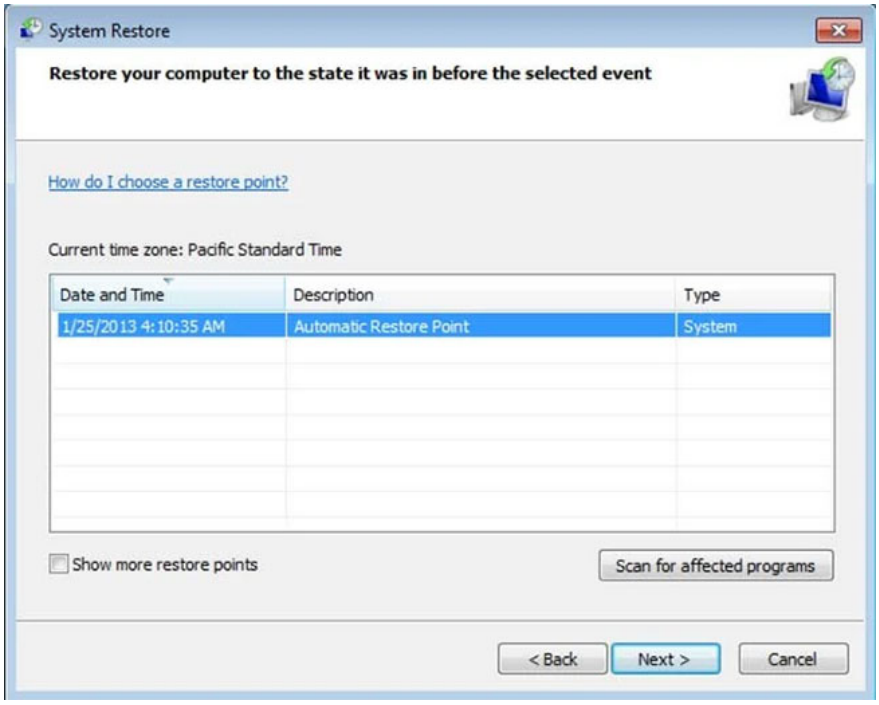
3. Next, enter this line: `rstrui.exe`and press `ENTER`.

4. In the window that opens, click **Next.**



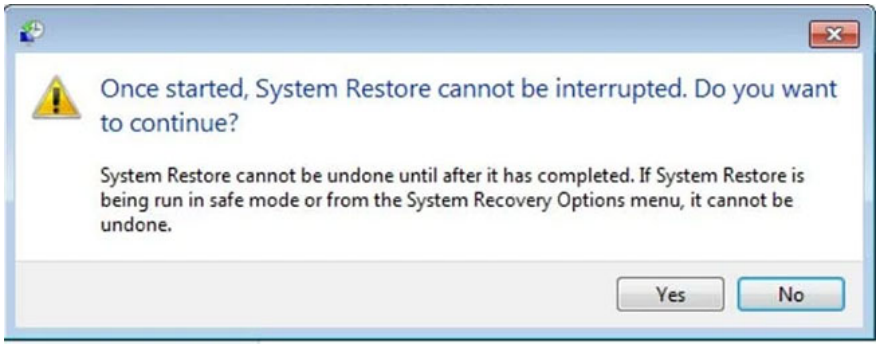
Click on Next

5. Select one of the Restore Points (available restore points) and click **Next.** This will restore the computer system to the time before the Moba ransomware entered the PC.



Select one of the Restore Points (available restore points).

6. In the window that opens, click **Yes.**

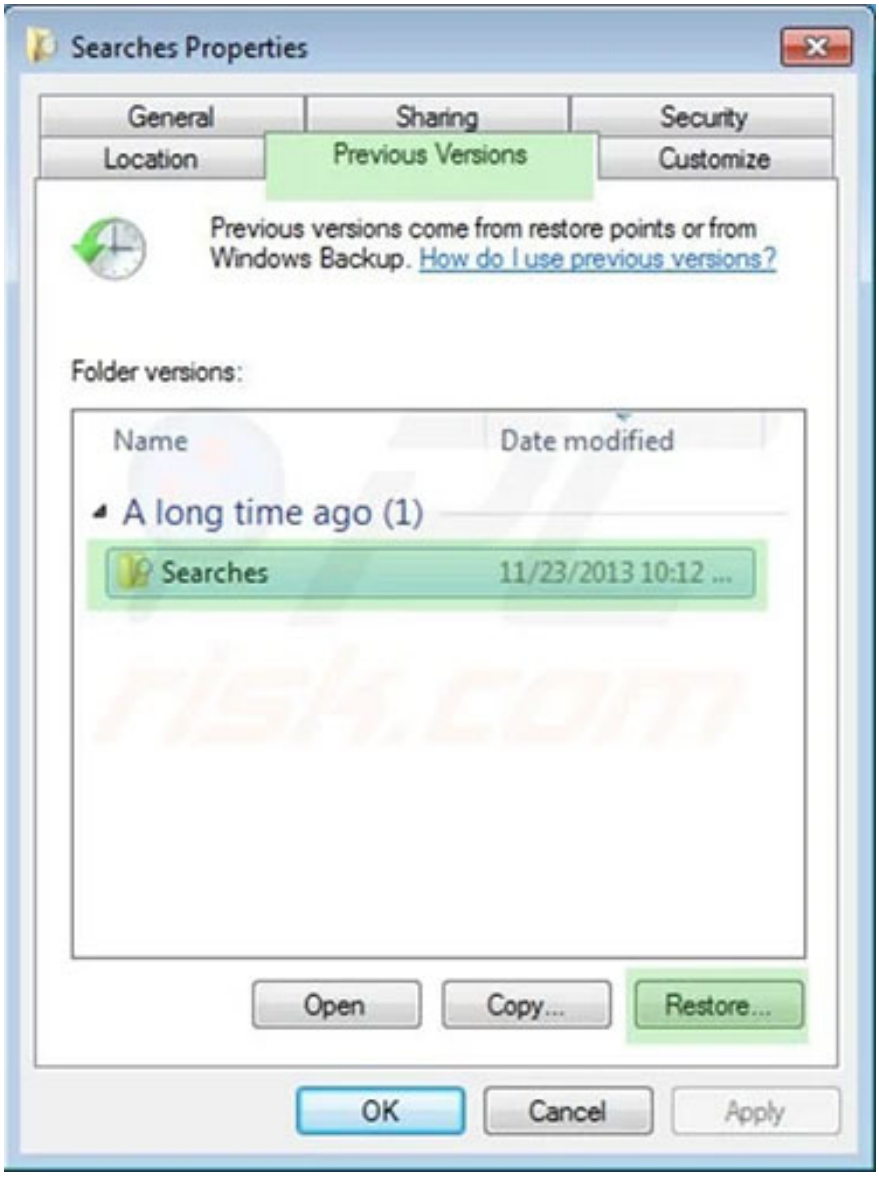


Click on Yes

7. After restoring the computer to a previous day, download and scan your PC with the software recommended above to remove any remaining Moba ransomware files.

To restore individual files encrypted with this ransomware, try using the **Windows Previous Versions feature** . This method is only effective if the System Restore function is enabled on the infected operating system. Note that some variants of Moba are known to remove **Shadow Volume Copies** of files, so this method may not work on all computers.

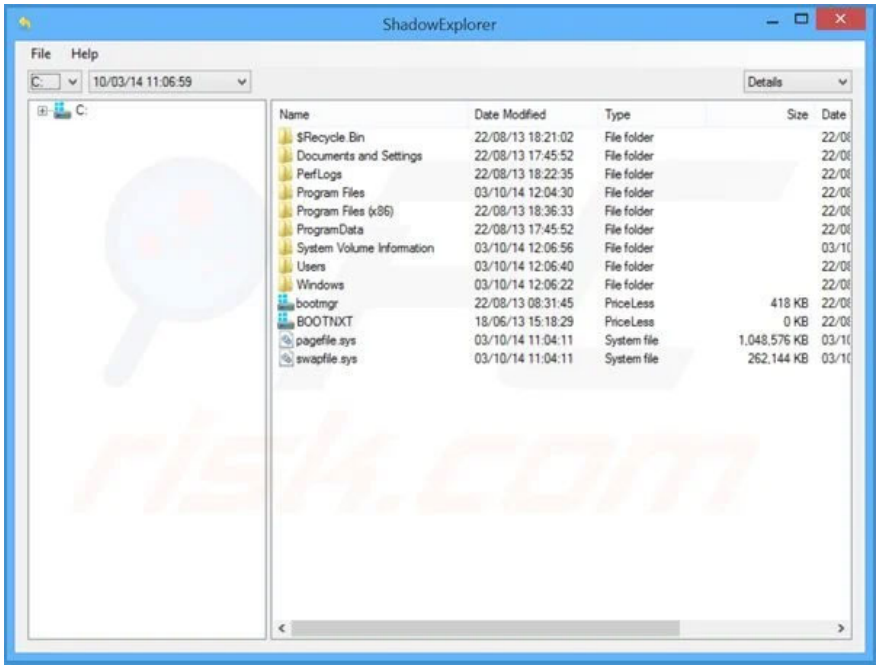
To restore a file, right-click on the file, select **Properties** and go to the **Previous Versions** tab . If the related file has Restore Point, select the file and click the **Restore** button **.**



Click the Restore button

If you cannot boot the computer in Safe Mode with Networking (or with Command Prompt), start the computer with a rescue disk. Some variants of ransomware may disable Safe Mode, making its removal complicated. To perform this step, you need to have access to another computer.

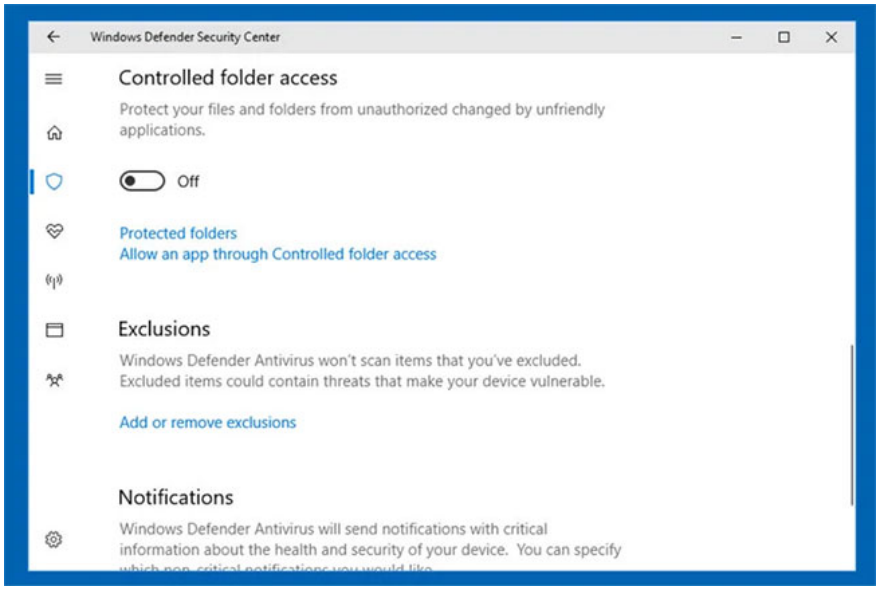
To regain control of the files encrypted by Moba, you can also try using a program called Shadow Explorer. To protect your computer from encrypted ransomware like this, use reputable anti-virus and anti-spyware programs.



Shadow Explorer

If you want to add an additional protection, you can use programs like HitmanPro.Alert and EasySync CryptoMonitor, to bring Group Policy Objects into the Registry to prevent phishing programs like Moba ransomware.

Note that the Windows 10 Fall Creators Update includes **Controlled Folder Access** , which blocks ransomware file encryption attempts. By default, this feature automatically protects files stored in **Documents, Pictures, Videos, Music, Favorites,** and **Desktop** folders . Windows 10 users should install this update to protect their data from ransomware attacks.



The Windows 10 Fall Creators Update includes Controlled Folder Access, which blocks ransomware file encryption attempts

Besides. The best way to avoid damage from ransomware infection is to maintain regular backups.

You finished reading the article "**How to remove Moba ransomware from the operating system**" 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.