

# How to protect your computer from Maoloo ransomware

The Maoloo ransomware is specifically designed to encrypt all important data files in order to extort money from victims. So, how can you protect your computer from Maoloo ransomware?

**Maoloo ransomware** is developed by cybercriminals with the sole purpose of extorting ransom from victims. See below for more details on what Maoloo ransomware is and how to protect your computer from it.



## How to protect your computer from Maoloo ransomware.

### Table of Contents:

1. What is Maoloo ransomware? 2.
- How does Maoloo ransomware attack? 3.
- How to protect your computer from Maoloo ransomware .
4. Other methods .

### *1. What is Maoloo ransomware?*

Maoloo ransomware is classified as a dangerous file-locking ransomware capable of encrypting users' valuable files and deleting system backups, forcing users to pay for their files over a specified period.

The primary purpose behind the Maolua ransomware is to extort money from users by preventing them from accessing, using, or modifying personal files stored on their systems until a ransom is paid.

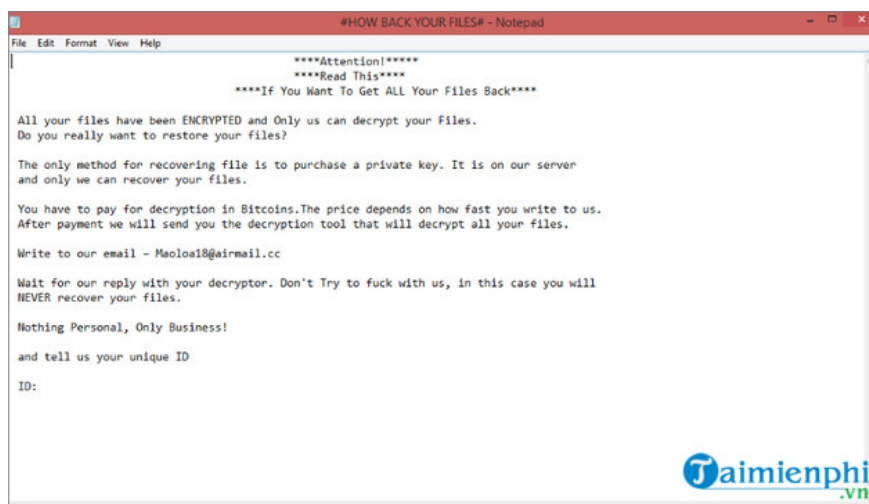


The Maolua ransomware encrypts all types of files and folders stored on a user's computer , **including text, music, images, work documents, PDFs, backup files, configuration files, etc.** Instead of directly locking files, Maolua changes the encrypted filename by adding the **.Maolua** extension to the filename.

In addition, you can also refer to "What is Ransomware?" to learn more about this malware and how to protect your computer from Ransomware here.

For example, a file named Music.jpg will be encoded and renamed to Music.Maolua by Maolua.

Whenever a user attempts to open these locked files, a ransom message will appear on the screen containing the text **#HOW BACK YOUR FILES#.txt** , including information about cryptocurrency and instructions on how to pay the ransom using Bitcoin or other cryptocurrencies.



However, even if the user/victim contacts the cybercriminals and pays the ransom, it is very difficult to crack the AES/DES ransomware Maolua, which generates unique decryption keys. In other words, using any key will not

yield the desired result. Furthermore, the cybercriminals store these keys on remote servers and are the only ones who can access them.

## ***2. How does Maoloo ransomware attack?***

Currently, Maoloo ransomware attacks target PC users worldwide. Maoloo distributes itself through various forms and mechanisms, typically including spam emails, third-party websites, torrents and peer-to-peer file sharing, free software (fake software updates), software cracks or piracy, and clickjacking.

In addition, the Maoloo ransomware also modifies Windows Registry entries to be able to survive and launch or block processes in the Windows environment. Such entries are often designed in a way that triggers the virus spontaneously every time Windows starts up.

Cybercriminals use these threats to steal users' personal data such as IP addresses, search URLs, browsing history, search queries, usernames, IDs, passwords, banking information, and ATM card information .

## ***3. How to protect your computer from Maoloo ransomware***

There have been cases where users have been attacked by the same Maoloo ransomware a second time, even after paying the ransom.

Therefore, if your computer is attacked by the Maoloo ransomware, instead of paying the ransom, you can follow the steps below to remove this ransomware:

**Step 1:** Unlock your computer in Safe Mode.

**Step 2:** Perform a system restore.

Detailed steps to follow:

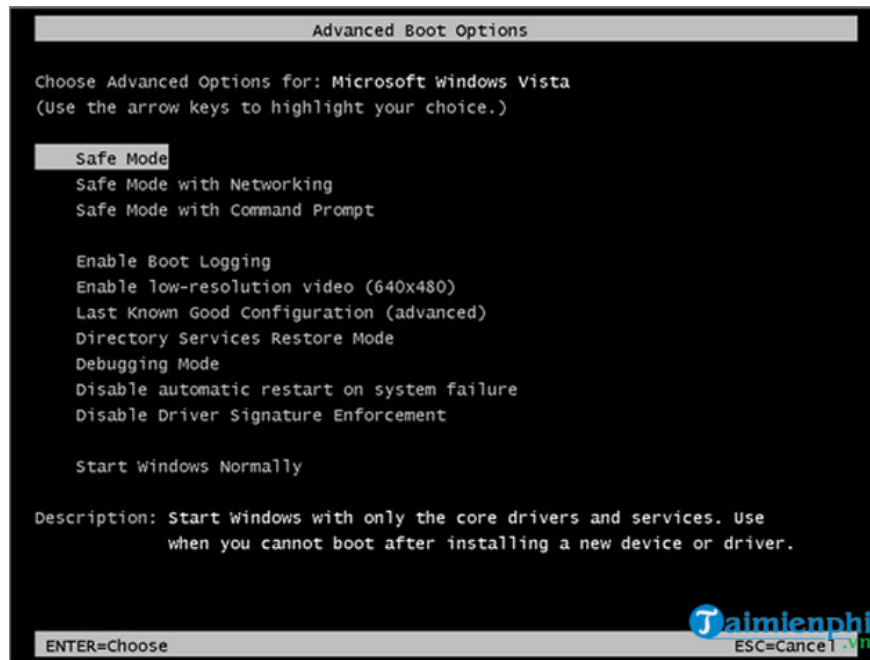
***Temporarily disable the Maoloo ransomware in Safe Mode via Command Prompt.***

**- For Windows 7**

**Step 1:** Click the **Start button => Shut down => Restart.**

**Step 2:** Press and hold the F8 key repeatedly while the computer is booting up to display advanced boot options.

**Step 3:** **Here, find and select the Safe mode with Command prompt option .**



## - For Windows 8 and 10

**Step 1:** On the login screen, click the Power option.

**Step 2:** Simultaneously press and hold **the Shift key** on your keyboard, then click **Restart**.

**Step 3 :** Next, find and click **Troubleshoot** , then select Advanced options, Startup settings, and finally click **Restart**.



**Step 4:** After the computer finishes booting, a list of boot options will appear on the screen. Find and click on **Enable Safe Mode with Command Prompt**.

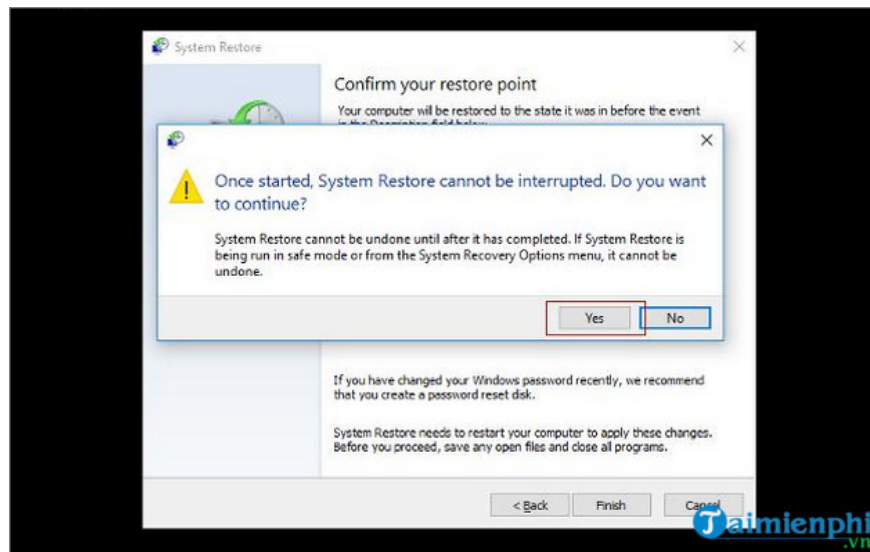
**Step 5: Perform system restore.**

In the Command Prompt window, enter the following command and press Enter:

**CD**

Next, enter the command **rstrui.exe** and press **Enter** again.

A new pop-up window will then appear on the screen. Click to select a restore point before your computer was infected with the Maoloo ransomware, then click **Yes**.



For more details on how to back up and restore your Windows 7, 8, and 10 system, please refer to this link.

#### 4. Other methods

- **Activate ad and pop-up blockers:** Ads and pop-ups on websites are the most common tactics used by cybercriminals to spread malware. Therefore, you should avoid clicking on unverified pages, software providers, pop-ups, etc., and install ad blockers for Chrome, Mozilla, and IE.
- **Regularly update to the latest version of Windows:** Also, don't forget to update your system regularly.
- **Limit third-party installations:** Avoid downloading and installing free third-party software. This is because software installation packages may include viruses and malware.
- **Regular backups:** Perform regular and periodic backups to ensure your data is safe, even in the event of a system infection with viruses or other malware.
- **Install antivirus software:** Finally, TipsMake recommends that you install effective antivirus software to comprehensively upgrade your system and avoid attacks from the Maoloo ransomware.

Above, TipsMake has shared and guided you on some ways **to protect your computer from the Maoloo ransomware**. Additionally, if you have any further questions, please leave your comments in the section below the article.

You finished reading the article "**How to protect your computer from Maoloo ransomware**" 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.

