.lockymap Files Virus (PyLocky Ransomware) – Remove and Restore Data

sensorstechforum.com/lockymap-files-virus-pylocky-ransomware-remove-restore-data/

Ventsislav Krastev September 3, 2018

This article is made with the goal of explaining what is the **.lockymap PyLocky ransomware** virus and how you can remove it from Windows plus how you can restore files, encrypted by it on your PC.

A new ransomware virus, going by the name of **PyLocky ransomware** has been detected to infect actively and encrypt files on the computers infected by it. The **.lockymap variant of PyLocky ransomware** then adds a ransom note whose main goal is to show you how you can pay a hefty ransom in order to get the cyber-criminals to recover your files. In the event that your computer has been infected by **PyLocky ransomware** virus, we recommend that you read this article as it will help you to remove this ransomware from your PC and restore your files.

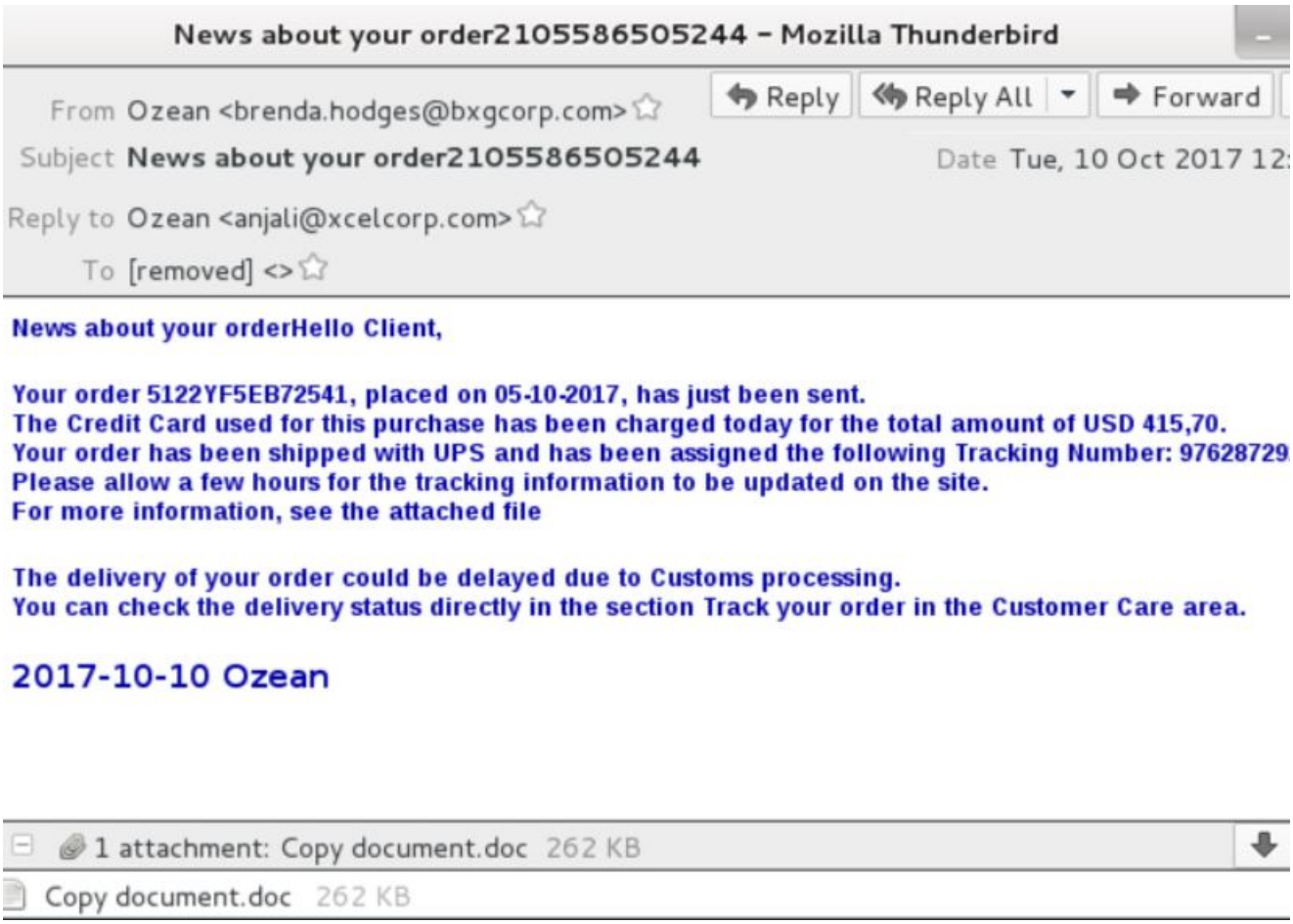
Threat Summary

Name	.lockymap Ransomware
Type	Ransomware, Cryptovirus
Short Description	Files are encrypted and the virus leaves a ransom note extorting victims to pay ransom in order to get their files to work once again.
Symptoms	The files on your computer have the **.lockymap** extension added to them and cannot be opened.
Distribution Method	Spam Emails, Email Attachments, Executable files

Detection Tool	See If Your System Has Been Affected by malware Download Malware Removal Tool
User Experience	Join Our Forum to Discuss .lockymap Ransomware.
Data Recovery Tool	Windows Data Recovery by Stellar Phoenix Notice! This product scans your drive sectors to recover lost files and it may not recover 100% of the encrypted files, but only few of them, depending on the situation and whether or not you have reformatted your drive.

PyLocky .lockymap Ransomware – Distribution

In order to infect a certain computer, the **.lockymap** files virus may be embedded as an attachment in a spam e-mail sent to you by the cyber-criminals themselves or via a spam bot. This e-mail may contain deceptive tactics to convince you that the attachment should immediately be opened:



Besides via e-mail, the PyLocky ransomware virus may also use other methods of infection. The crooks may upload the infection file in compromised WordPress sites, that may pretend as if they offer different programs the user needs for free download, such as:

- Software installers.
- Portable versions of programs.
- Cracks.
- A patch.
- License activation software.
- Keygens.

PyLocky .lockymap Ransomware – Analysis

Once the .lockymap ransomware virus has already infected your computer, the ransomware may start to download and run it's payload. The payload of PyLocky ransomware, consists of several files, the main of which has the following information:

→ Name: facture_4739149_08.26.2018.exe
SHA256:8655f8599b0892d55efc13fea404b520858d01812251b1d25dcf0afb4684dce9
Size: 5.3 MB

In addition to the main infection file, other files may also be dropped on the victim's computer and they are likely located in the following directories:

- %Temp%
- %AppData%
- %Local%
- %LocalLow%
- %Roaming%

Among the files dropped on the user's computer is also the ransom note file, called **LOCKY-README.txt** file. It has the following contents:

> Please be adviced:
>
> All your files, pictures document and data has been encrypted with Military Grade Encryption RSA ABS-256.
> Your information is not lost. But Encrypted.
>
> In order for you to restore your files you have to purchase Decrypter.
>
> Follow this steps to restore your files.
>
> 1* Download the Tor Browser. (Just type in google “Download Tor“
>
> 2‘ Browse to URL : https://4wcgqlckaazungm.onion/index.php
>
> 3* Purchase the Decryptor to restore your files.
>
> It is very simple. If you don’t believe that we can restore your files, then you can restore 1 file of image format for free.
> Be aware the time is ticking. Price will be doubled every 96 hours so use it wisely.
>
> Your unique ID :
>
> CAUTION:
>
> Please do not try to modify or delete any encrypted file as it will be hard to restore it.
>
> SUPPORT:
>
> You can contact support to help decrypt your files for you.
>
> Click on support at https://4wcgqlckaazungm.onion/index.php

In addition to this, the PyLocky ransomware may also modify the Windows Registry Editor, primarily the Run and RunOnce registry sub-keys of it, creating values in them with the location of the malicious .exe file of PyLocky. This may ultimately result in the malicious files running automatically when you log in Windows:

→ HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

But this is not all that happens after infection with **PyLocky ranomware**, because the virus may also modify the volume shadow copies of the infected computer by executing the following commands:

→ sc stop VVS
sc stop wscsvc
sc stop WinDefend
sc stop wuauserv
sc stop BITS
sc stop ERSvc
sc stop WerSvc
cmd.exe /C bcdedit /set {default} recoveryenabled No
cmd.exe /C bcdedit /set {default} bootstatuspolicy ignoreallfailures
C:\Windows\System32\cmd.exe" /C vssadmin.exe Delete Shadows /All /Quiet

These commands may result in the .lockymap file version of PyLocky to delete all of the files you have backed up on your computer.

.lockymap PyLocky Virus – Encryption Process

The .lockymap variant of PyLocky virus may scan for the following types of files on your PC, after it infects it:

→ "PNG .PSD .PSPIMAGE .TGA .THM .TIF .TIFF .YUV .AI .EPS .PS .SVG .INDD .PCT .PDF .XLR .XLS .XLSX .ACCDB .DB .DBF .MDB .PDB .SQL .APK .APP .BAT .CGI .COM .EXE .GADGET .JAR .PIF .WSF .DEM .GAM .NES .ROM .SAV CAD Files .DWG .DXF GIS Files .GPX .KML .KMZ .ASP .ASPX .CER .CFM .CSR .CSS .HTM .HTML .JS .JSP .PHP .RSS .XHTML. DOC .DOCX .LOG .MSG .ODT .PAGES .RTF .TEX .TXT .WPD .WPS .CSV .DAT .GED .KEY .KEYCHAIN .PPS .PPT .PPTX ..INI .PRF Encoded Files .HQX .MIM .UUE .7Z .CBR .DEB .GZ .PKG .RAR .RPM .SITX .TAR.GZ .ZIP .ZIPX .BIN .CUE .DMG .ISO .MDF .TOAST .VCD SDF .TAR .TAX2014 .TAX2015 .VCF .XML Audio Files .AIF .IFF .M3U .M4A .MID .MP3 .MPA .WAV .WMA Video Files .3G2 .3GP .ASF .AVI .FLV .M4V .MOV .MP4 .MPG .RM .SRT .SWF .VOB .WMV 3D .3DM .3DS .MAX .OBJ R.BMP .DDS .GIF .JPG ..CRX .PLUGIN .FNT .FON .OTF .TTF .CAB .CPL .CUR .DESKTHEMEPACK .DLL .DMP .DRV .ICNS .ICO .LNK .SYS .CFG"

After this, the ransomware may encrypt the files, setting two different file extensions – **.lockedfile and .lockymap**. The encrypted files start to appear like the following:

Picture.bmp.lockymap

Picture.png.lockedfile

Remove PyLocky Ransomware and Restore .lockymap Files

For the removal of this ransomware virus, we would suggest that you follow the removal instructions underneath this article. They have been created with the main purpose of allowing manual and automatic removal methods. If the manual removal steps do not help you or you cannot fully remove **PyLocky** by yourself, then researchers strognly recommend to download an advanced anti-malware program for the removal. Such software will completely and effectively remove **PyLocky** from your computer and make sure that it is protected from all sorts of advanced threats in the future as well.

If you wish to restore .lockedfile and .lockymap files encrypted by PyLocky ransowmare, we suggest that you try ot the alternative methods for file recovery in step **“2. Restore files, encrypted by .lockymap Ransomware”**. They may not be 100% effective to restore all of them but some of them may be able to recover a portion of the files.

Ventsislav Krastev

Ventsislav is a cybersecurity expert at SensorsTechForum since 2015. He has been researching, covering, helping victims with the latest malware infections plus testing and reviewing software and the newest tech developments. Having graduated Marketing as well, Ventsislav also has passion for learning new shifts and innovations in cybersecurity that

become game changers. After studying Value Chain Management, Network Administration and Computer Administration of System Applications, he found his true calling within the cybersecrurity industry and is a strong believer in the education of every user towards online safety and security.

More Posts - Website

Follow Me:

Previous post

Next post

Attention! SensorsTechForum strongly recommends that all malware victims should look for assistance only by reputable sources. Many guides out there claim to offer free recovery and decryption for files encrypted by ransomware viruses. Be advised that **some of them may only be after your money**.
As a site that has been dedicated to providing free removal instructions for ransomware and malware since 2014, SensorsTechForum's recommendation is to **only pay attention to trustworthy sources**.

How to recognize trustworthy sources:

- Always check "About Us" web page.
- Profile of the content creator.
- Make sure that real people are behind the site and not fake names and profiles.

OFFER
REMOVE IT NOW (PC)
with Anti-Malware
We recommend you to download SpyHunter and run **free scan to remove all virus files on your PC**. This saves you hours of time and effort compared to doing the removal yourself. *SpyHunter 5 free remover allows you, subject to a 48-hour waiting period, one remediation and removal for results found. Read EULA and Privacy Policy*

- Guide 1: How to Remove .lockymap Ransomware from Windows.
- Guide 2: Get rid of .lockymap Ransomware from Mac OS X.

Windows Mac OS X

How to Remove .lockymap Ransomware from Windows.

Step 1: Boot Your PC In Safe Mode to isolate and remove .lockymap Ransomware

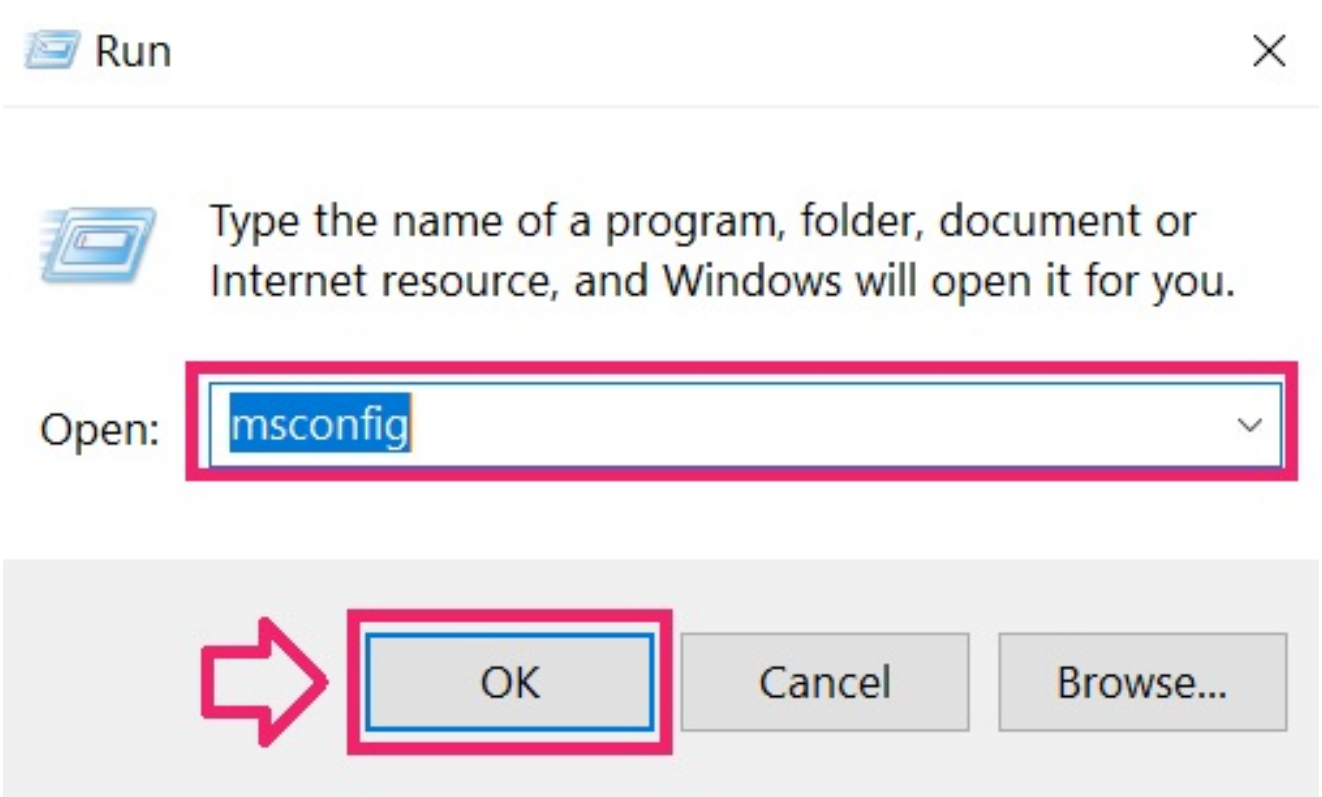
OFFER
Manual Removal Usually Takes Time and You Risk Damaging Your Files If Not Careful!
We Recommend To Scan Your PC with SpyHunter
Keep in mind, that SpyHunter's scanner is only for malware detection. If SpyHunter detects malware on your PC, you will need to purchase SpyHunter's malware removal tool to remove the malware threats. Read our SpyHunter 5 review. Click on the corresponding links to check SpyHunter's EULA, Privacy Policy and Threat Assessment Criteria

---

1. Hold Windows key(⊞) **+ R**

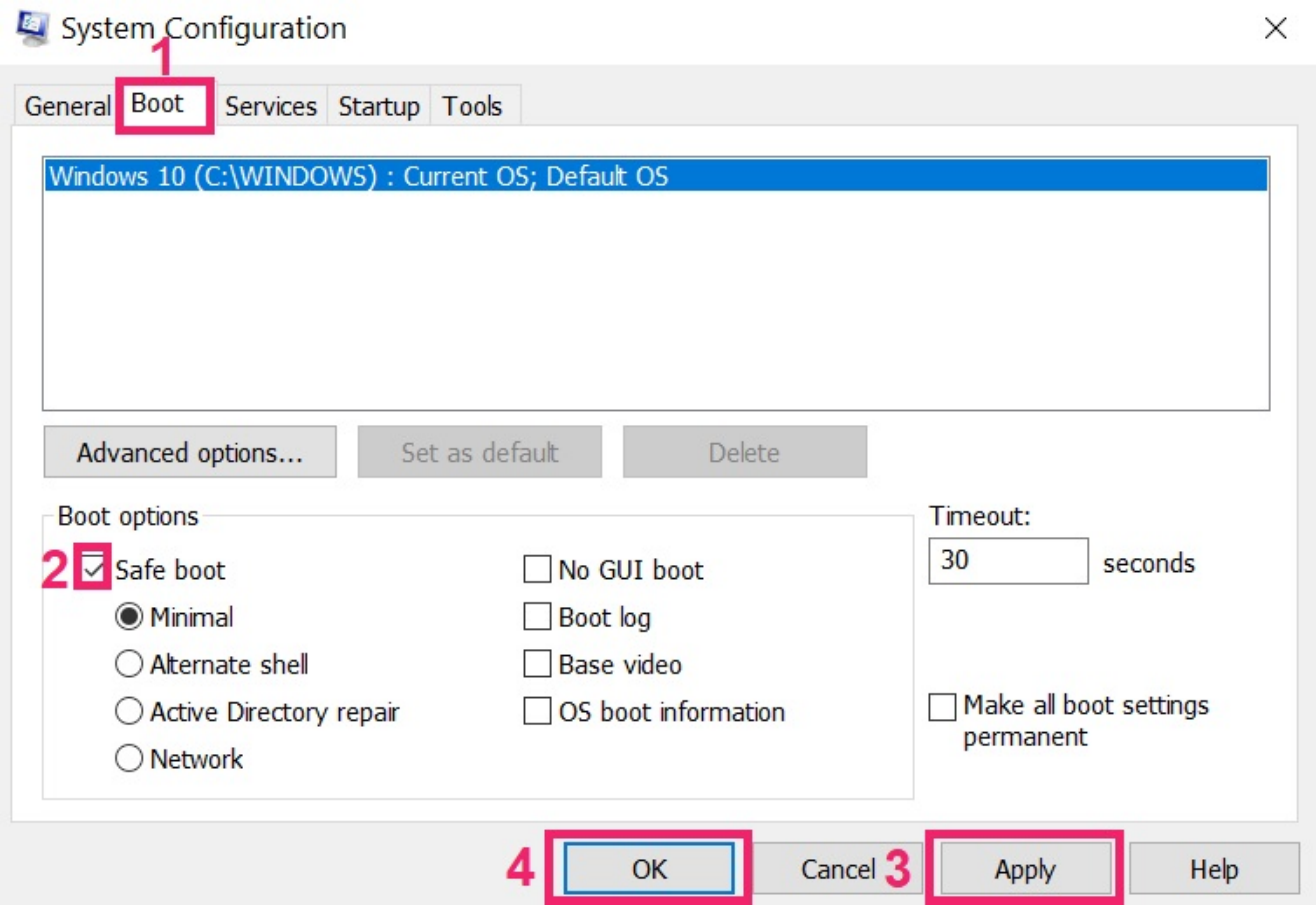
---

2. The "**Run**" Window will appear. In it, type "**msconfig**" and click **OK**.



---

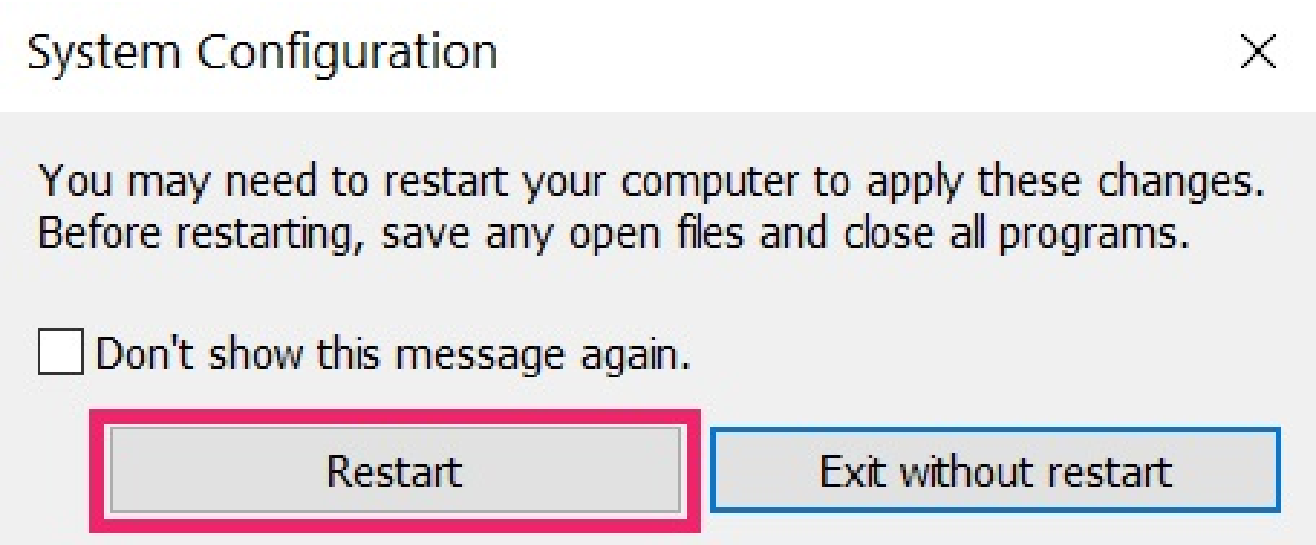
3. Go to the **"Boot"** tab. There select **"Safe Boot"** and then click **"Apply"** and **"OK"**.



Tip: Make sure to reverse those changes by unticking Safe Boot after that, because your system will always boot in Safe Boot from now on.

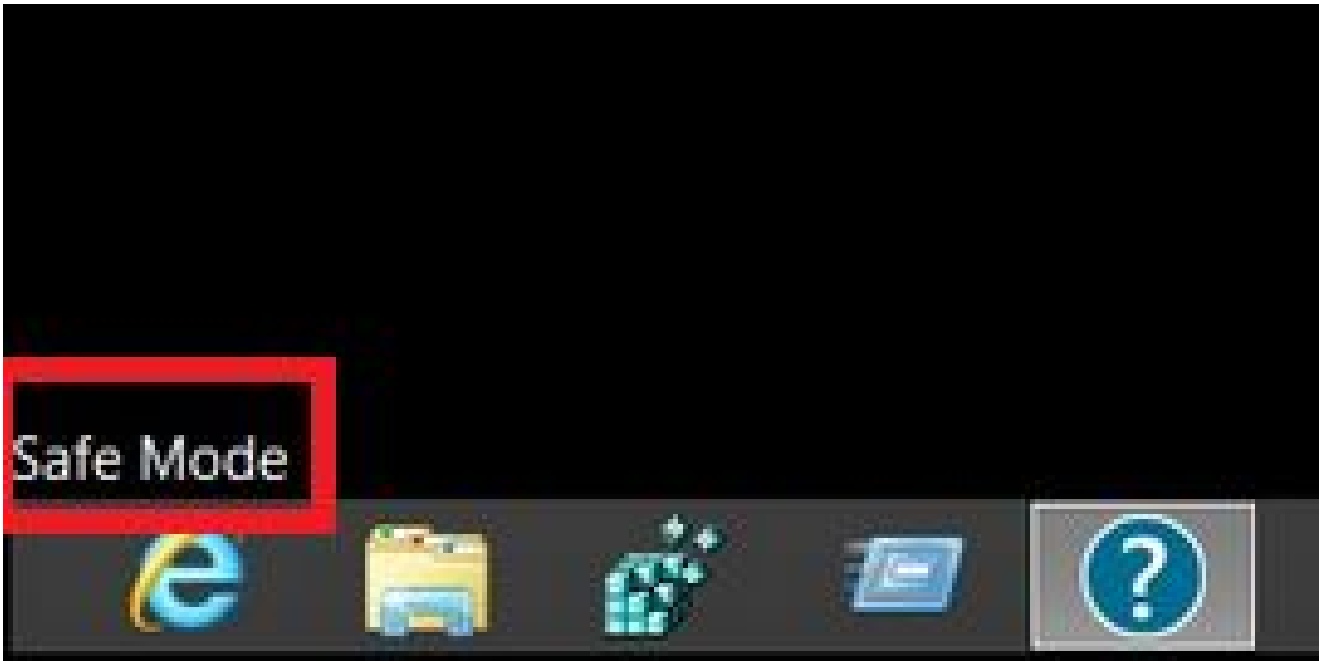
---

4. When prompted, click on "**Restart**" to go into Safe Mode.



---

5. You can recognise Safe Mode by the words written on the corners of your screen.



Step 2: Uninstall .lockymap Ransomware and related software from Windows

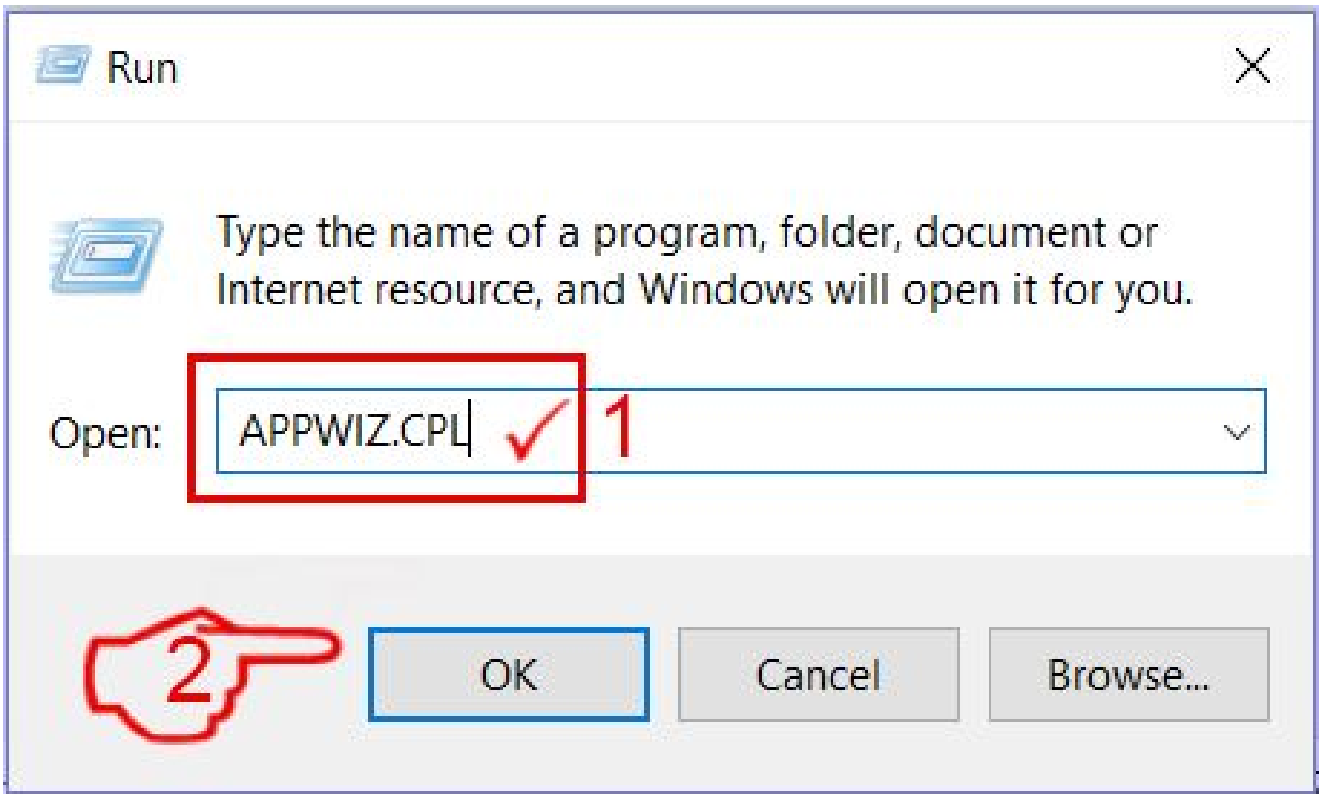
Here is a method in few easy steps that should be able to uninstall most programs. No matter if you are using Windows 10, 8, 7, Vista or XP, those steps will get the job done. Dragging the program or its folder to the recycle bin can be a **very bad decision**. If you do that, bits and pieces of the program are left behind, and that can lead to unstable work of your PC, errors with the file type associations and other unpleasant activities. The proper way to get a program off your computer is to Uninstall it. **To do that:**

---

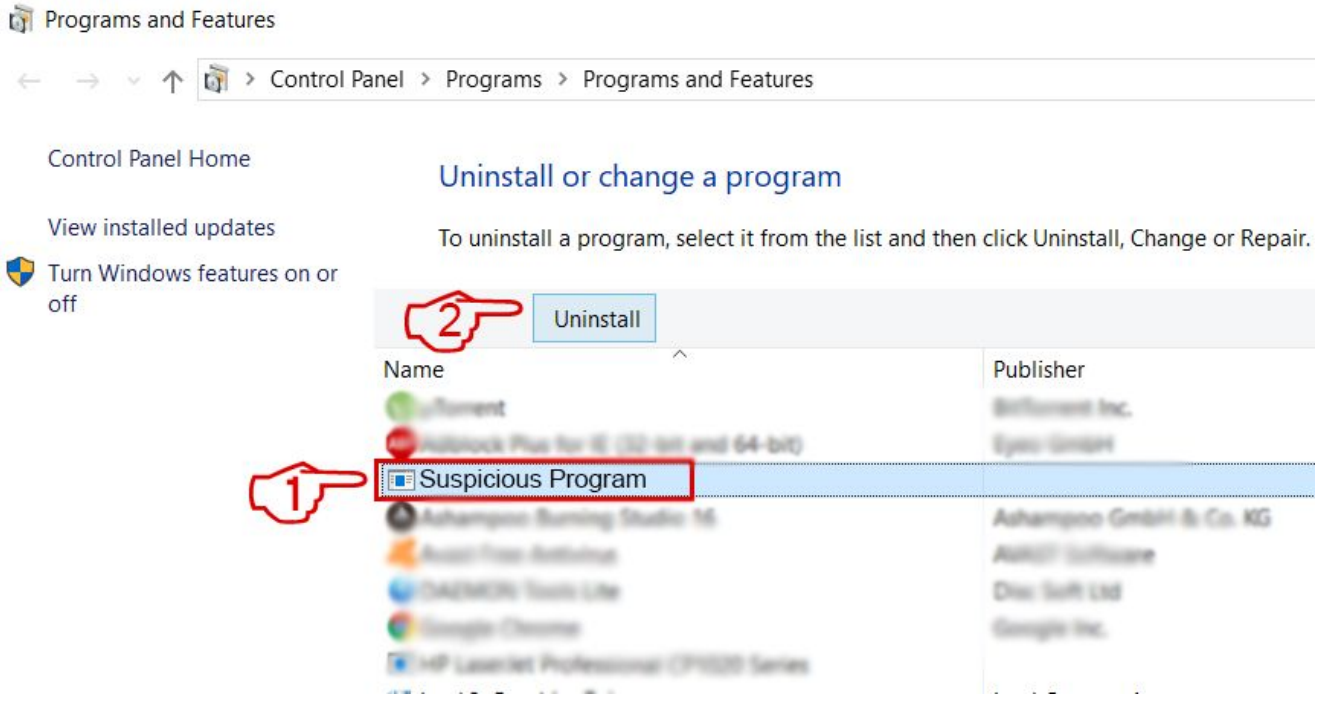
1. Hold the **Windows Logo Button** and "**R**" on your keyboard. A Pop-up window will appear.

---

2. In the field type in "**appwiz.cpl**" and press **ENTER**.



3. This will open a window with all the programs installed on the PC. Select the program that you want to remove, and press "**Uninstall**"



Follow the instructions above and you will successfully uninstall most programs.

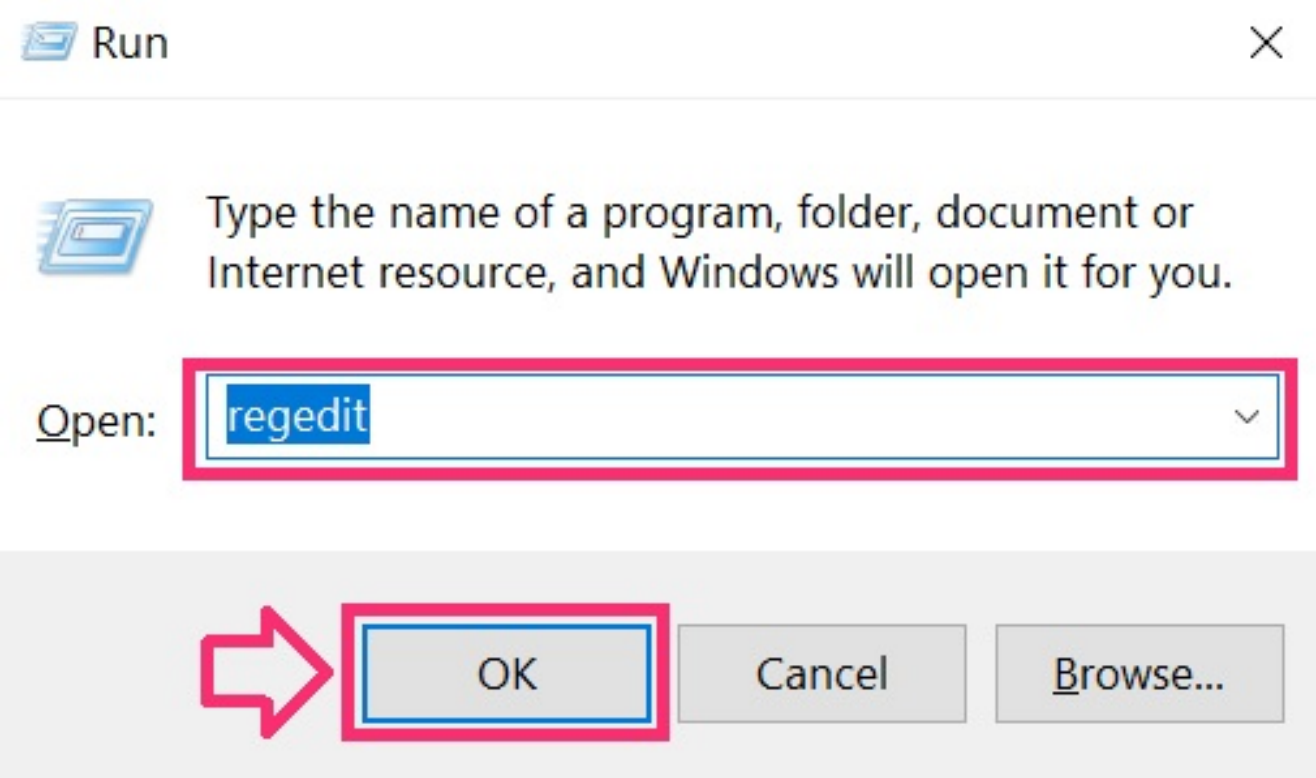
Step 3: Clean any registries, created by .lockymap Ransomware on your computer.

The usually targeted registries of Windows machines are the following:

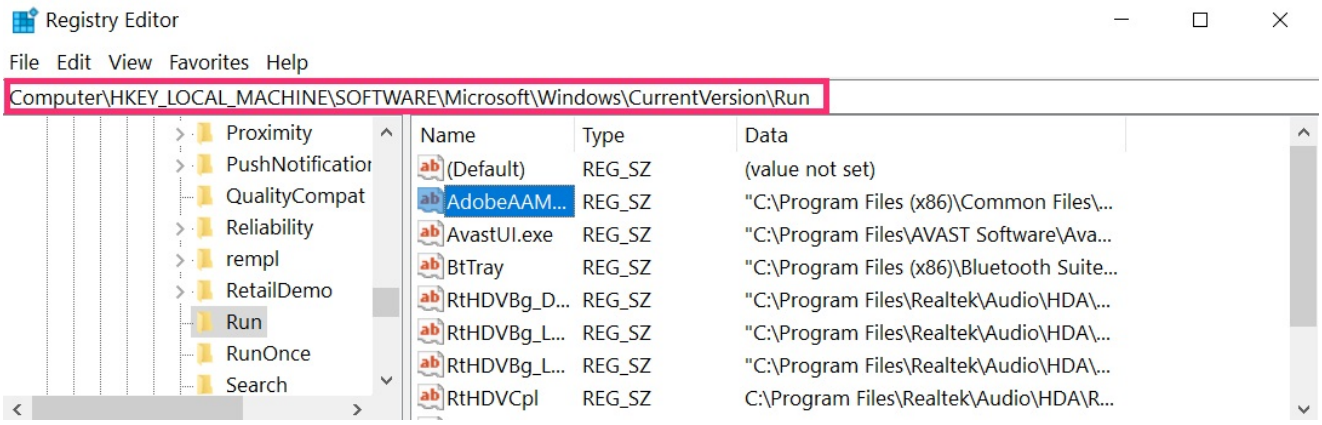
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

You can access them by opening the Windows registry editor and deleting any values, created by .lockymap Ransomware there. This can happen by following the steps underneath:

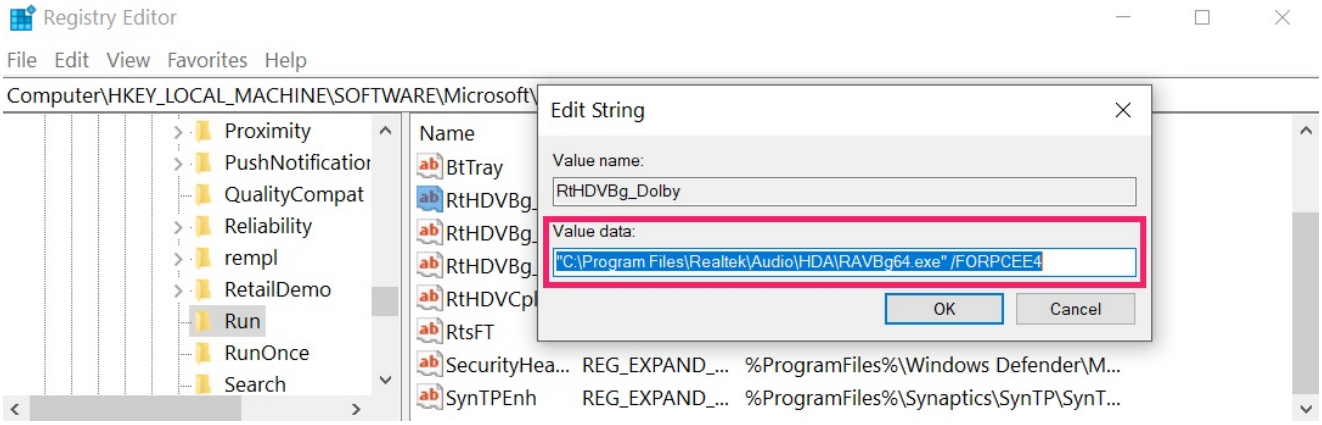
1. Open the **Run Window** again, type **"regedit"** and click **OK**.



2. When you open it, you can freely navigate to the *Run and RunOnce* keys, whose locations are shown above.



3. You can remove the value of the virus by right-clicking on it and removing it.



*Tip: To find a virus-created value, you can right-click on it and click **"Modify"** to see which file it is set to run. If this is the virus file location, remove the value.*

IMPORTANT!

*Before starting **"Step 4"**, please **boot back into Normal mode**, **in case you are currently in Safe Mode**.*

*This will enable you to install and **use SpyHunter 5 successfully**.*

Step 4: Scan for .lockymap Ransomware with SpyHunter Anti-Malware Tool

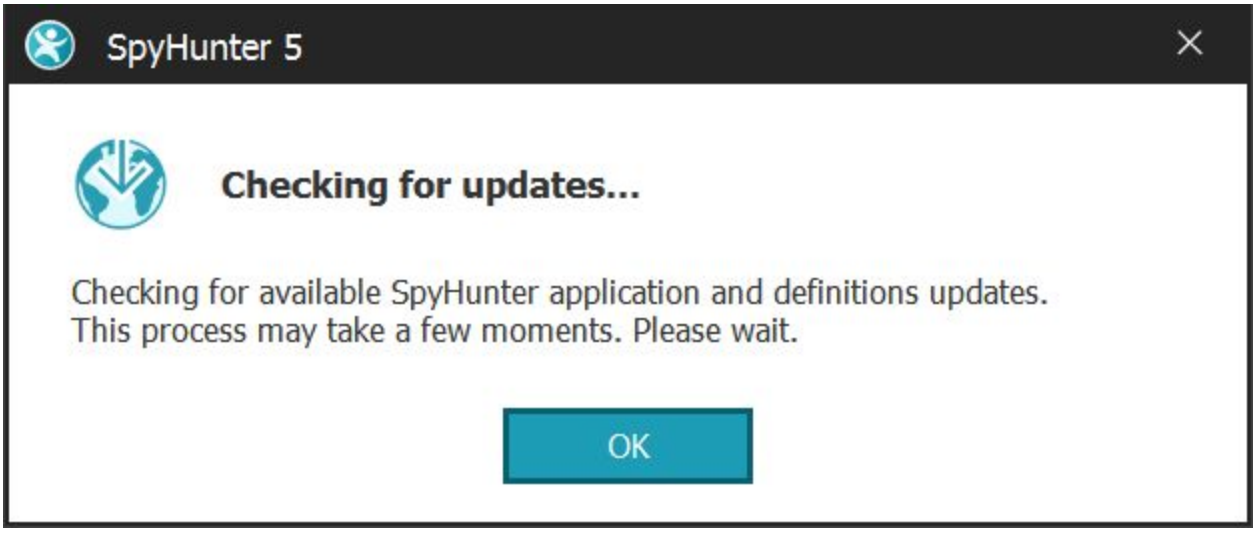
1. Click on the "Download" button to proceed to SpyHunter's download page.

Download

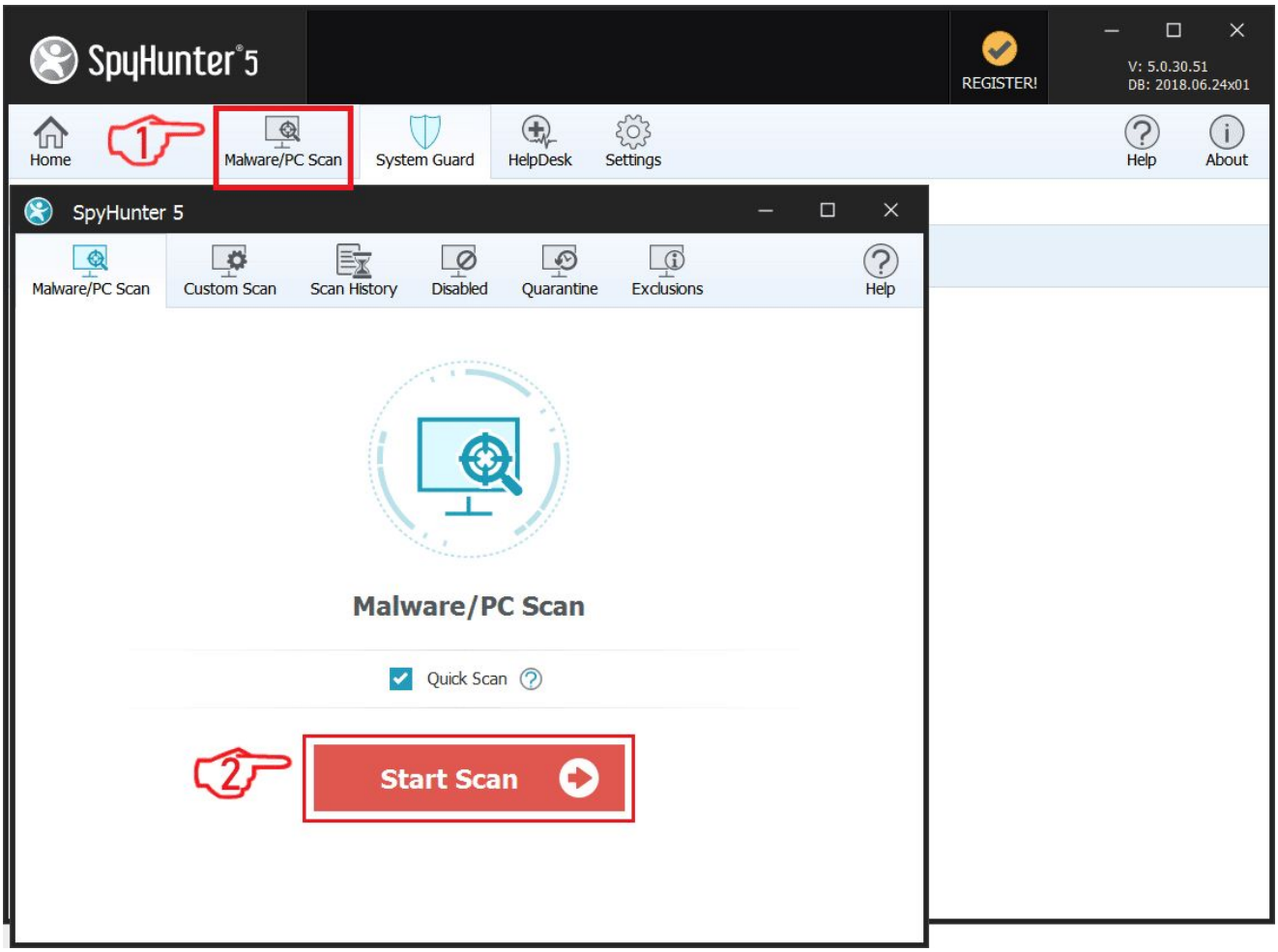
Malware Removal Tool

It is recommended to run a scan before purchasing the full version of the software to make sure that the current version of the malware can be detected by SpyHunter. Click on the corresponding links to check SpyHunter's EULA, Privacy Policy and Threat Assessment Criteria.

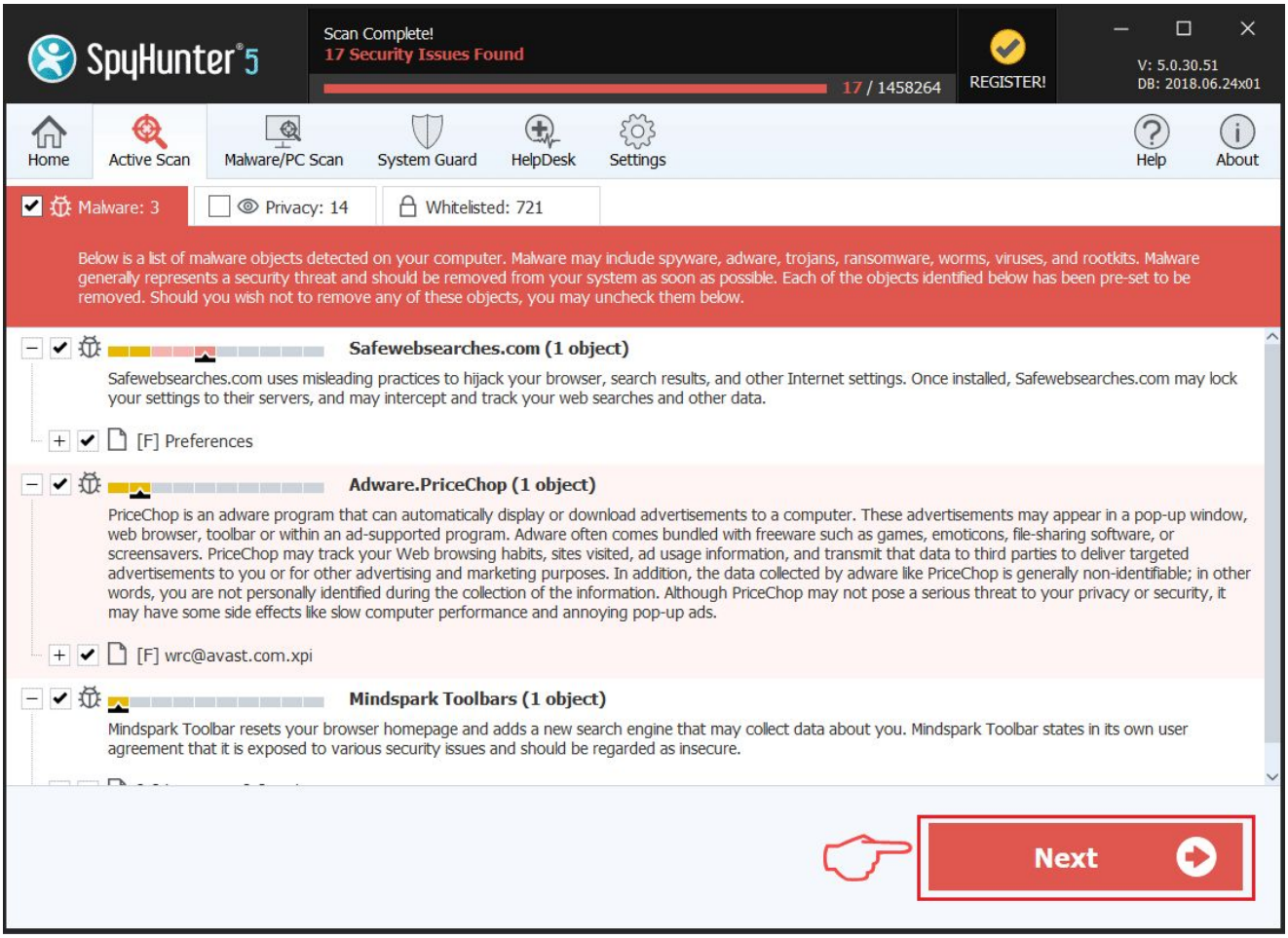
2. After you have installed SpyHunter, wait for it to **update automatically**.



3. After the update process has finished, click on the **'Malware/PC Scan'** tab. A new window will appear. Click on **'Start Scan'**.



4. After SpyHunter has finished scanning your PC for any files of the associated threat and found them, you can try to get them removed automatically and permanently by clicking on the **'Next'** button.



If any threats have been removed, it is highly recommended to **restart your PC**.
Step 5 (Optional): Try to Restore Files Encrypted by .lockymap Ransomware.

Ransomware infections and .lockymap Ransomware aim to encrypt your files using an encryption algorithm which may be very difficult to decrypt. This is why we have suggested a data recovery method that may help you go around direct decryption and try to restore your files. Bear in mind that this method may not be 100% effective but may also help you a little or a lot in different situations.

1. Download the reccomended Data Recovery software by clicking on the link underneath:
EaseUS Data Recovery Software
Simply click on the link and on the website menus on top, choose **Data Recovery - Data Recovery Wizard** for Windows or Mac (depending on your OS), and then download and run the tool.

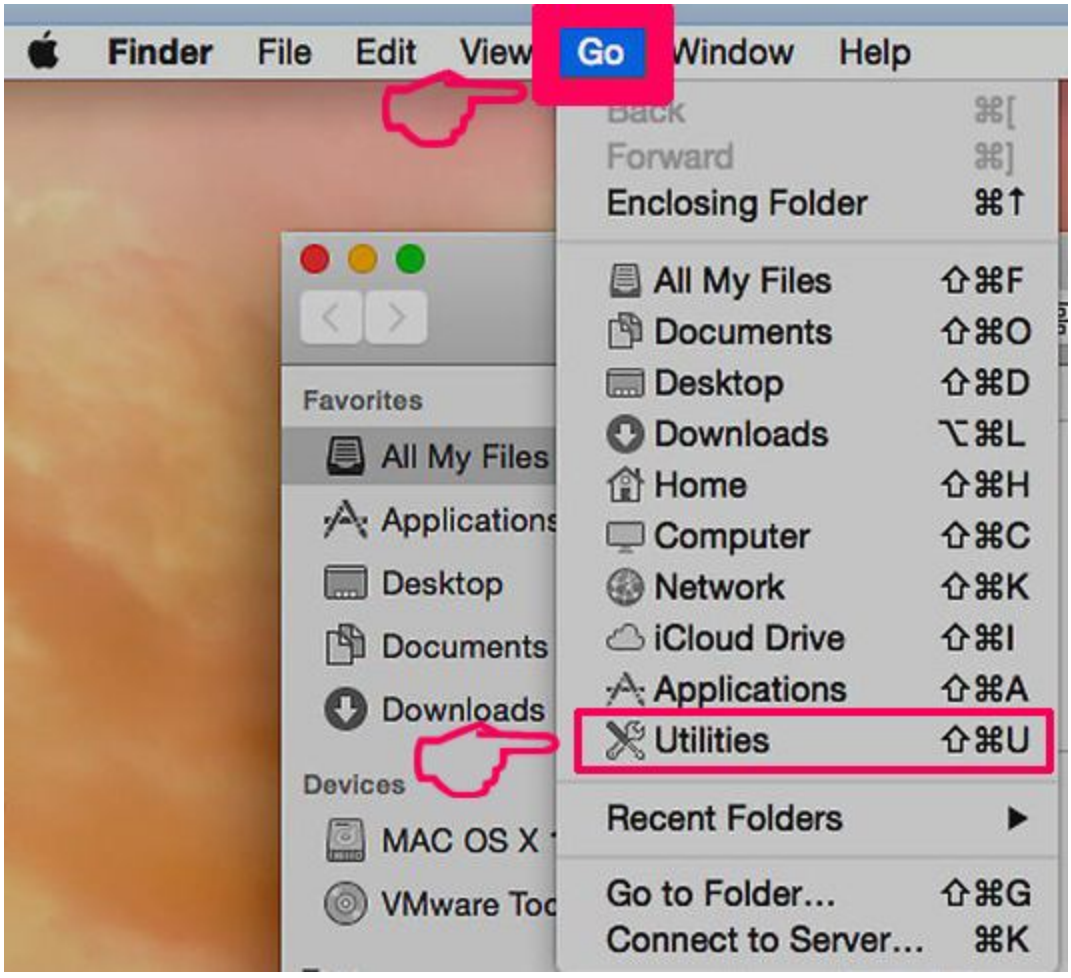
Windows Mac OS X

Get rid of .lockymap Ransomware from Mac OS X.

Step 1: Uninstall **.lockymap Ransomware** and remove related files and objects

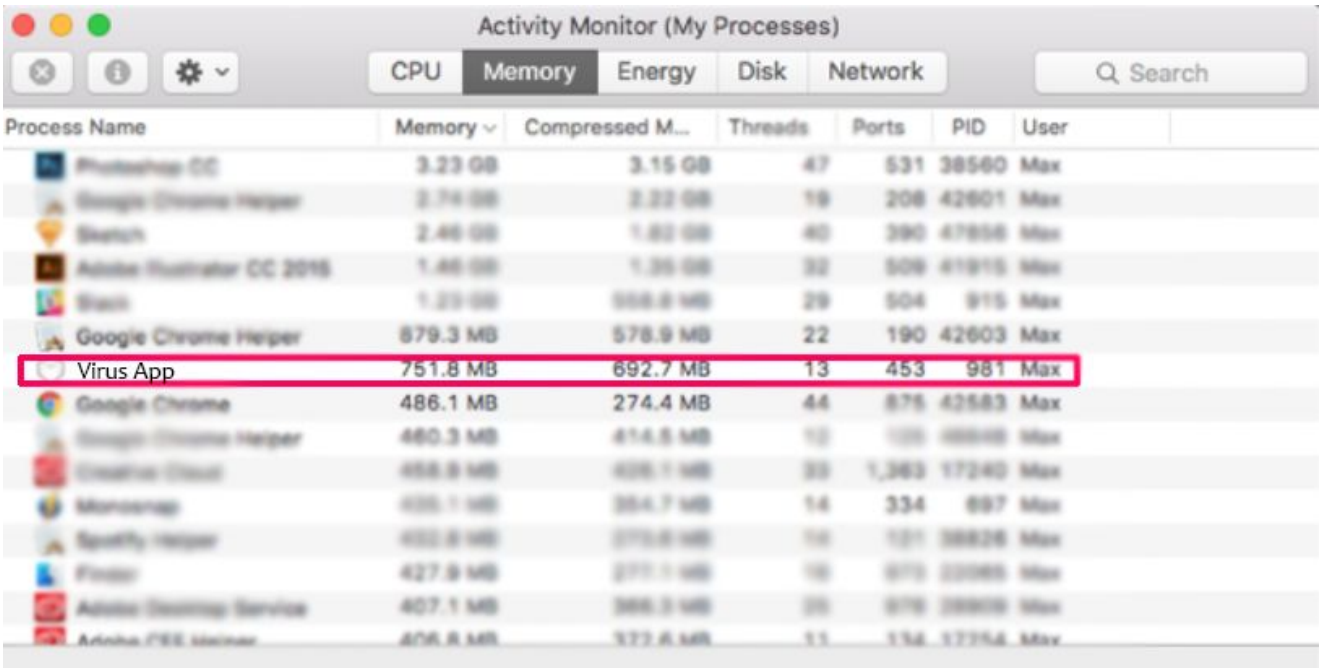
OFFER
Manual Removal Usually Takes Time and You Risk Damaging Your Files If Not Careful!
We Recommend To Scan Your Mac with SpyHunter for Mac
Keep in mind, that SpyHunter for Mac needs to purchased to remove the malware threats.
Click on the corresponding links to check SpyHunter's EULA and Privacy Policy

1. Hit the ⇧+⌘+**U** keys to open **Utilities**. Another way is to click on "**Go**" and then click "**Utilities**", like the image below shows:



2. Find **Activity Monitor** and double-click it:

3. In the Activity Monitor look for any suspicious processes, belonging or related to .lockymap Ransomware:



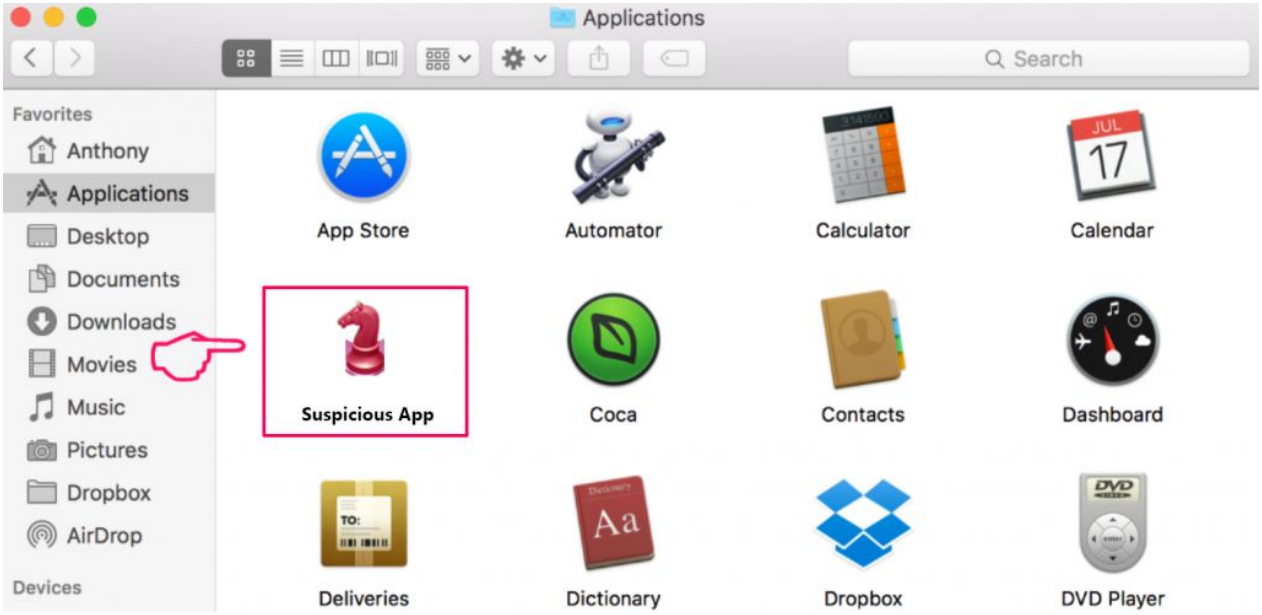
Tip: To quit a process completely, choose the “**Force Quit**” option.

---

4. Click on the "**Go**" button again, but this time select **Applications**. Another way is with the **⇧+⌘+A** buttons.

---

5. In the Applications menu, look for any suspicious app or an app with a name, similar or identical to .lockymap Ransomware. If you find it, right-click on the app and select “**Move to Trash**”.



6: Select Accounts, after which click on the Login Items preference. Your Mac will then show you a list of items that start automatically when you log in. Look for any suspicious apps identical or similar to .lockymap Ransomware. Check the app you want to stop from running automatically and then select on the Minus ("-") icon to hide it.

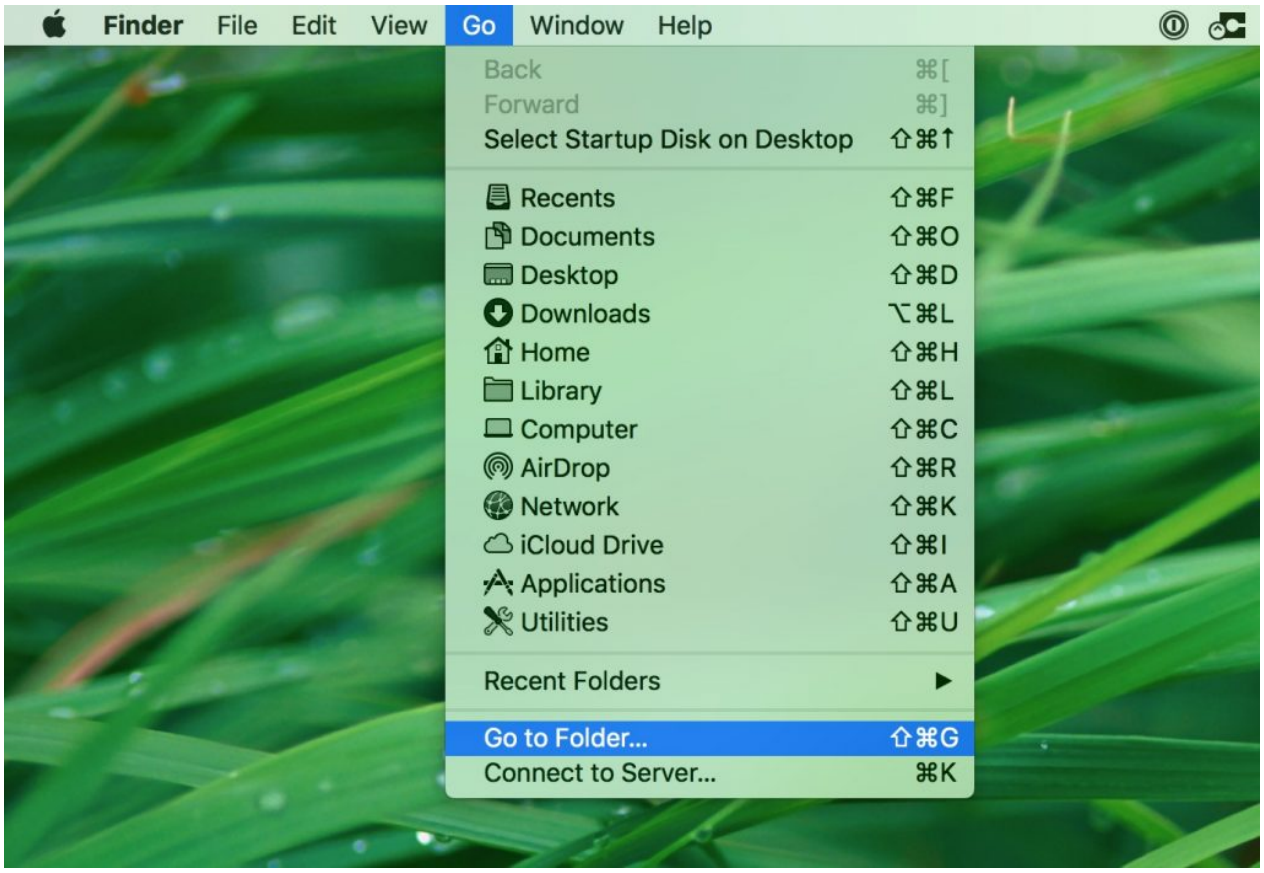
7: Remove any left-over files that might be related to this threat manually by following the sub-steps below:

- Go to **Finder**.
- In the search bar type the name of the app that you want to remove.
- Above the search bar change the two drop down menus to **"System Files"** and **"Are Included"** so that you can see all of the files associated with the application you want to remove. Bear in mind that some of the files may not be related to the app so be very careful which files you delete.
- If all of the files are related, hold the **⌘+A** buttons to select them and then drive them to **"Trash"**.

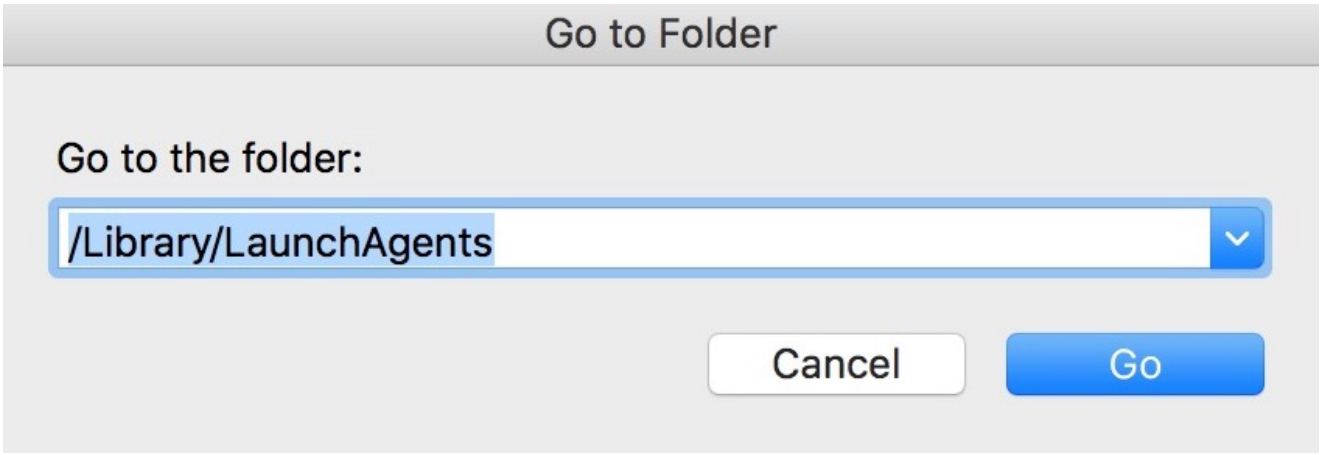
*In case you cannot remove .lockymap Ransomware via **Step 1** above:*

In case you cannot find the virus files and objects in your Applications or other places we have shown above, you can manually look for them in the Libraries of your Mac. But before doing this, please read the disclaimer below:

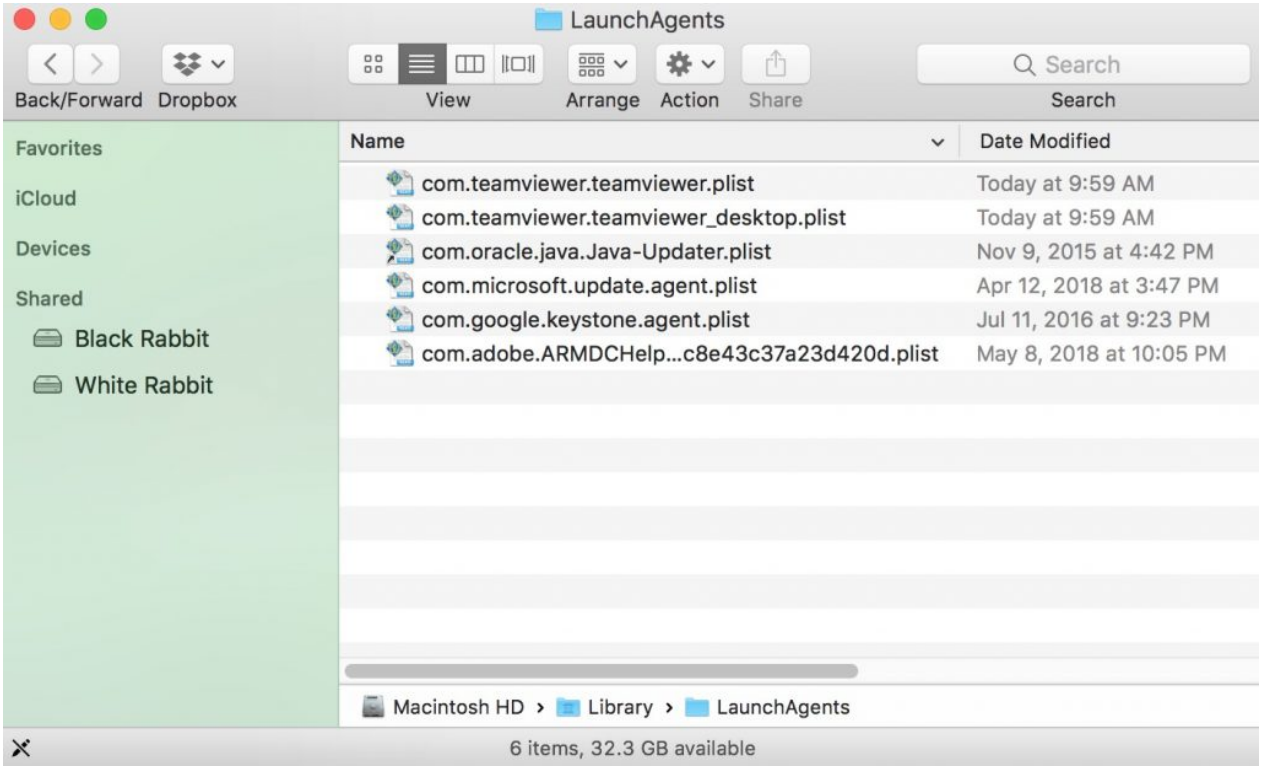
***Disclaimer!** If you are about to tamper with Library files on Mac, be sure to know the name of the virus file, because if you delete the wrong file, it may cause irreversible damage to your MacOS. Continue on your own responsibility!*
1: Click on **"Go"** and Then **"Go to Folder"** as shown underneath:



2: Type in "/Library/LauchAgents/" and click **Ok**:



3: Delete all of the virus files that have similar or the same name as .lockymap Ransomware. If you believe there is no such file, do not delete anything.

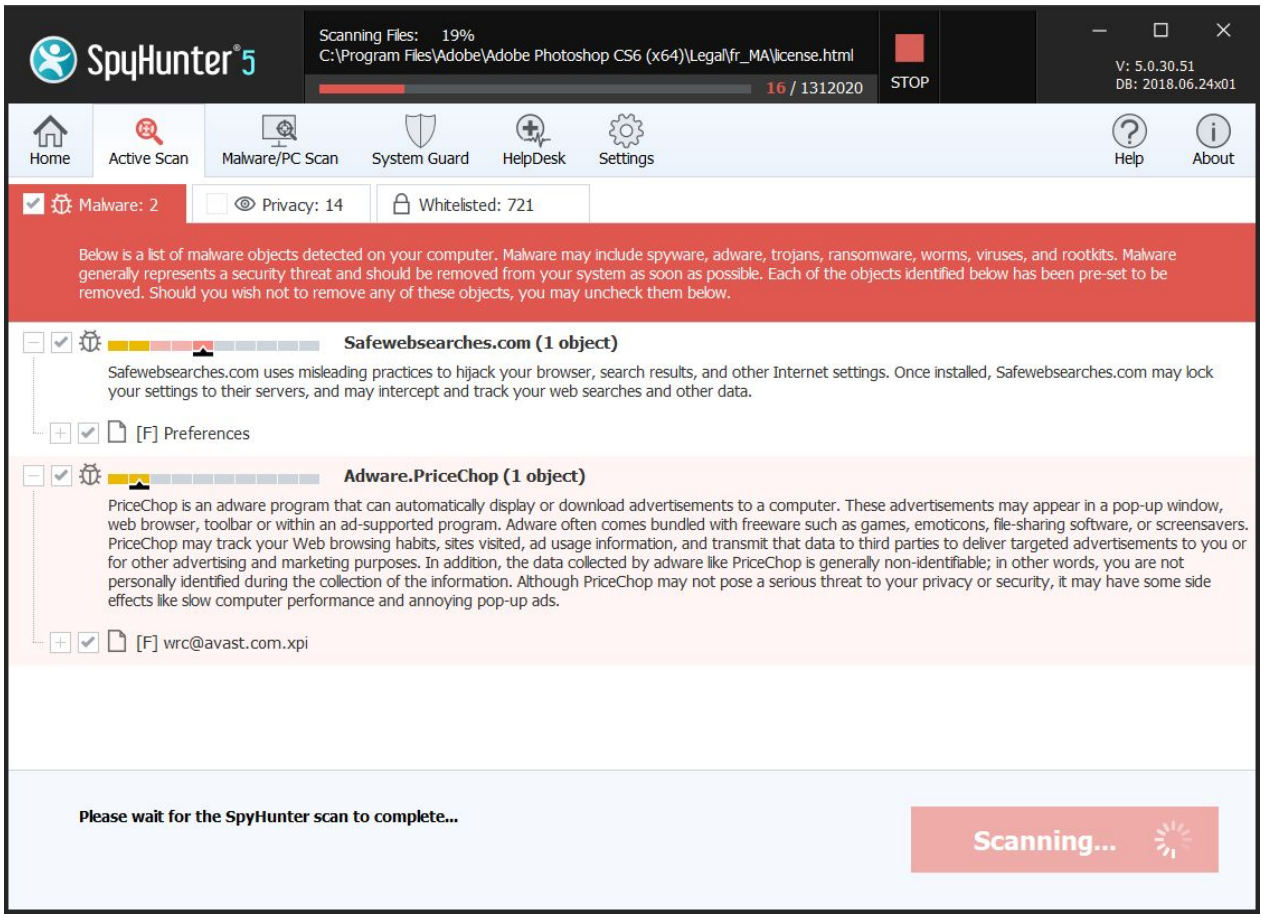


You can repeat the same procedure with the following other Library directories:

→ ~/Library/LaunchAgents
/Library/LaunchDaemons

> *Tip:* **~** *is there on purpose, because it leads to more LaunchAgents.*

Click **the button below** below to download **SpyHunter for Mac** and scan for .lockymap Ransomware:
Download
SpyHunter for Mac



Step 3 (Optional): Try to Restore Files Encrypted by .lockymap Ransomware.

Ransomware infections and .lockymap Ransomware aim to encrypt your files using an encryption algorithm which may be very difficult to decrypt. This is why we have suggested a data recovery method that may help you go around direct decryption and try to restore your files. Bear in mind that this method may not be 100% effective but may also help you a little or a lot in different situations.

1. Download the reccomended Data Recovery software by clicking on the link underneath:
EaseUS Data Recovery Software
Simply click on the link and on the website menus on top, choose **Data Recovery - Data Recovery Wizard** for Windows or Mac (depending on your OS), and then download and run the tool.

.lockymap Ransomware FAQ

What is .lockymap Ransomware ransomware and how does it work?

.lockymap Ransomware is a ransomware infection - the malicious software that enters your computer silently and blocks either access to the computer itself or encrypt your files.

Many ransomware viruses use sophisticated encryption algorithm how to make your files inaccessible. The goal of ransomware infections is to demand that you pay a ransom payment to get access to your files back.

How does .lockymap Ransomware ransomware infect my computer?

Via several ways..lockymap Ransomware Ransomware infects computers by being sent **via phishing e-mails, containing virus attachment**.

This attachment is usually masked as an important document, like an invoice, bank document or even a plane ticket and it looks very convincing to users.

After you **download and execute this attachment**, a drive-by download occurs and your computer is infected with the ransomware virus.

Another way, you may become a victim of .lockymap Ransomware is if you download a fake installer, crack or patch from a low reputation website or if you click on a virus link. Many users report getting a ransomware infection by downloading torrents.

How to open ..lockymap Ransomware files?

You can't. At this point the **..lockymap Ransomware** files are **encrypted**. You can only open them once they are decrypted.

Decryptor did not decrypt my data. What now?

Do not panic and **backup the file**s. If a decryptor did not decrypt your **..lockymap Ransomware** files successfully, then do not despair, because this virus is still new.

One way to restore files, encrypted by .lockymap Ransomware ransomware is to use a **decryptor** for it. But since it's a new virus, advised that the decryption keys for it may not be out yet and available to the public. We will update this article and keep you posted as soon as this decryptor is released.

How Do I restore "..lockymap Ransomware" files (Other Methods)?

Yes, sometimes files can be restored. We have suggested several **file recovery methods** that could work if you want to restore **..lockymap Ransomware** files.

These methods are in no way 100% guarantee that you will be able to get your files back. But if you have a backup, your chances of success are much greater.

How do I get rid of .lockymap Ransomware ransomware virus?

The safest way and the most efficient one for the removal of this ransomware infection is the use a **professional anti malware software**. It will scan for and locate .lockymap Ransomware ransomware and then remove it without causing any additional harm to your important ..lockymap Ransomware files.

Also, keep in mind that viruses like **.lockymap Ransomware ransomware** also install Trojans and keyloggers that can **steal your passwords and accounts**. Scanning your computer with an anti-malware software will make sure that all of these virus components are removed and your computer is protected in the future.

What to Do If nothing works?

There is still a lot you can do. If none of the above methods seem to work for you, then **try these methods**:

- Try to **find a safe computer** from where you can can login on your own line accounts like One Drive, iDrive, Google Drive and so on.
- Try to **contact your friends**, relatives and other people so that they can check if they have some of your important photos or documents just in case you sent them.
- Also, check if some of the files that were encrypted it can be **re-downloaded from the web**.
- Another clever way to get back some of your files is to **find another old computer, a flash drive or even a CD or a DVD** where you may have saved your older documents. You might be surprised what will turn up.
- You can also **go to your email account** to check if you can send any attachments to other people. Usually what is sent the email is saved on your account and you can re-download it. But most importantly, make sure that this is done from a safe computer and make sure to remove the virus first.

More tips you can find on our forums, where you can also asks any questions about your ransomware problem.

How to Report Ransomware to Authorities?

In case your computer got infected with a ransomware infection, you can report it to the local Police departments. It can help authorities worldwide track and determine the perpetrators behind the virus that has infected your computer. Below, we have prepared a list with government websites, where you can file a report in case you are a victim of a cybercrime:

Cyber-security authorities, responsible for handling ransomware attack reports in different regions all over the world:

- Germany - Offizielles Portal der deutschen Polizei
- United States - IC3 Internet Crime Complaint Centre
- United Kingdom - Action Fraud Police

- France - Ministère de l'Intérieur
- Italy - Polizia Di Stato
- Spain - Policía Nacional
- Netherlands - Politie
- Poland - Policja
- Portugal - Polícia Judiciária
- Greece - Cyber Crime Unit (Hellenic Police)
- India - Mumbai Police - CyberCrime Investigation Cell
- Australia - Australian High Tech Crime Center

Reports may be responded to in different timeframes, depending on your local authorities.