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

By Ventsislav Krastev

Published: 2018-09-03 · Archived: 2026-04-05 21:44:42 UTC

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.

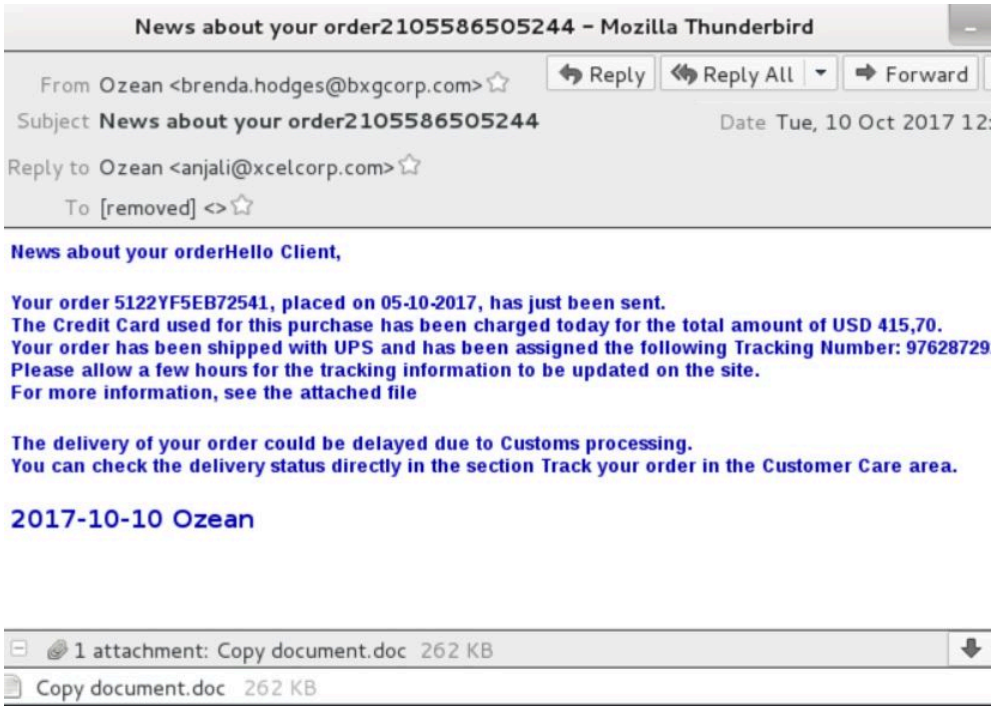
On this page:

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 Spy Hunter
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

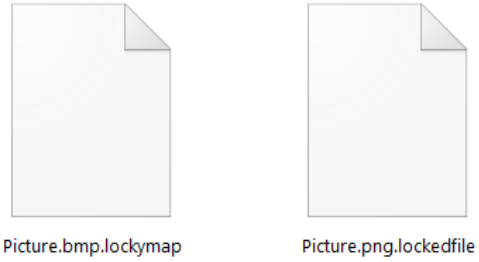
These commands may result in the .lockymap file version of PyLocky to delete all of the files you have backed up on your computer.

.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:



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 strongly 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.

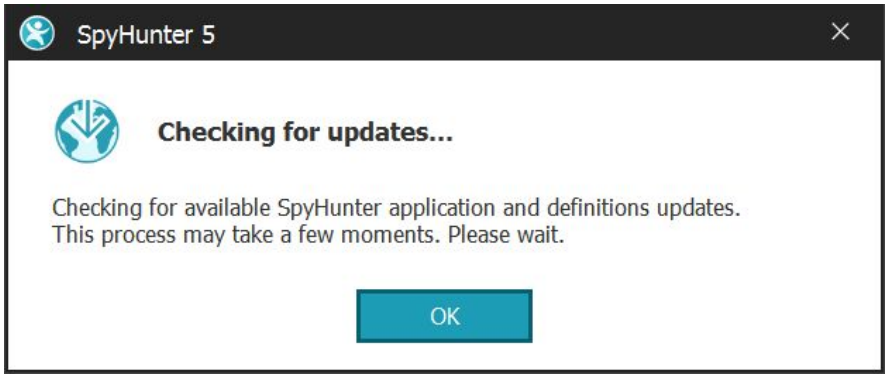
- Step 1
- Step 2
- Step 3
- Step 4
- Step 5

Step 1: Scan for .lockymap Ransomware with SpyHunter Anti-Malware Tool

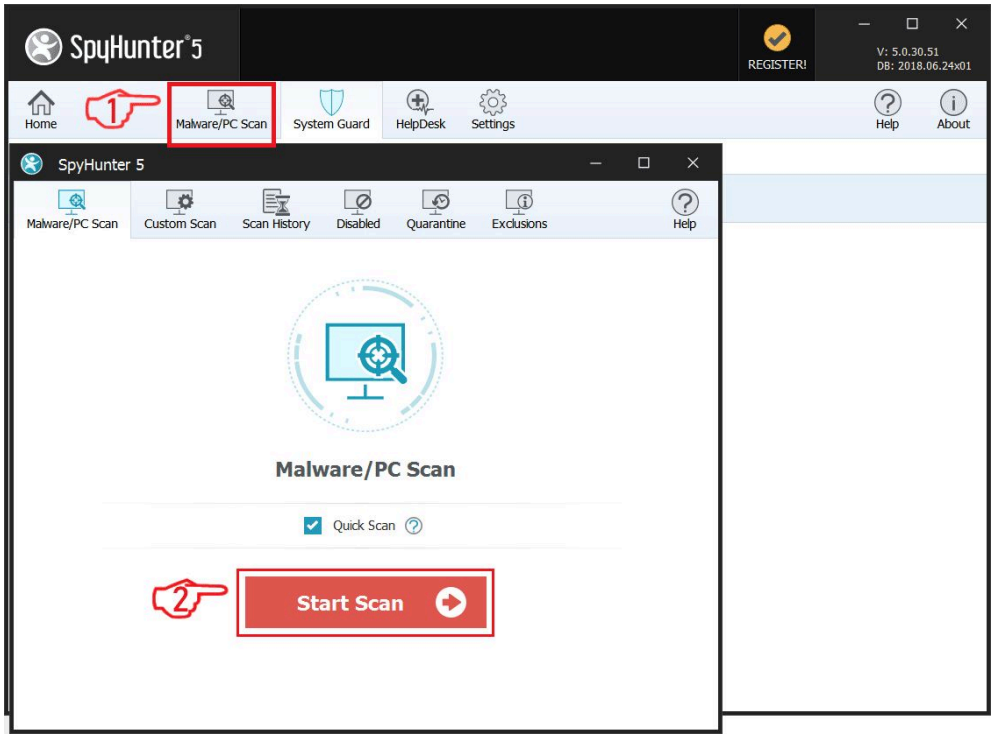
1. Click on the "Download" button to proceed to SpyHunter's download page.

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.

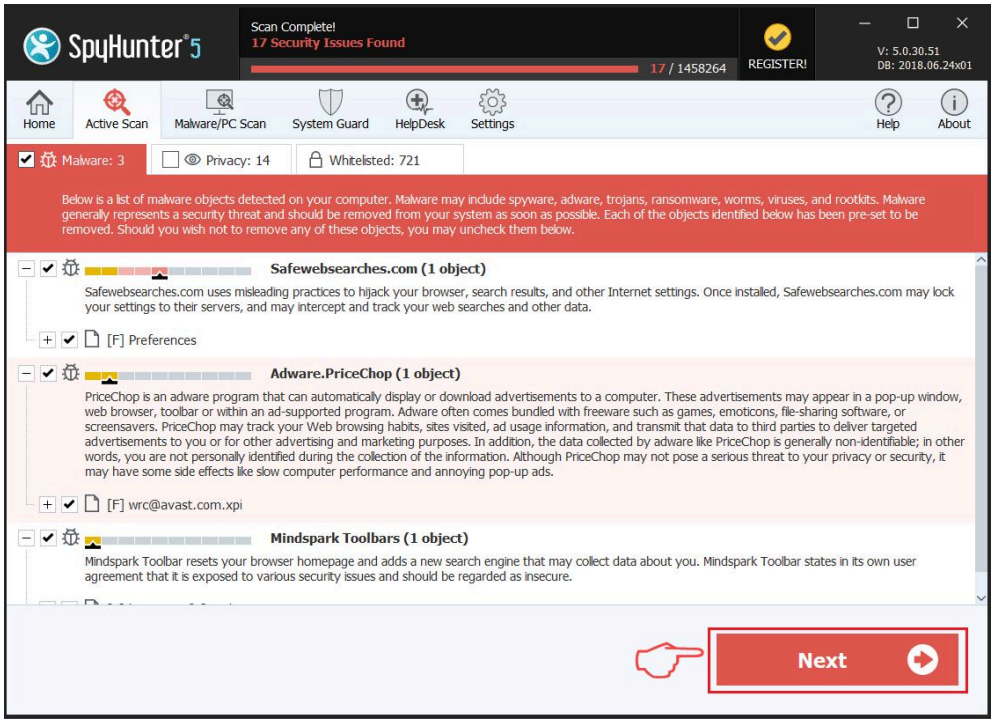
2. After you have installed SpyHunter, wait for it to update automatically.



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**.

Ransomware Automatic Removal - Video Guide

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

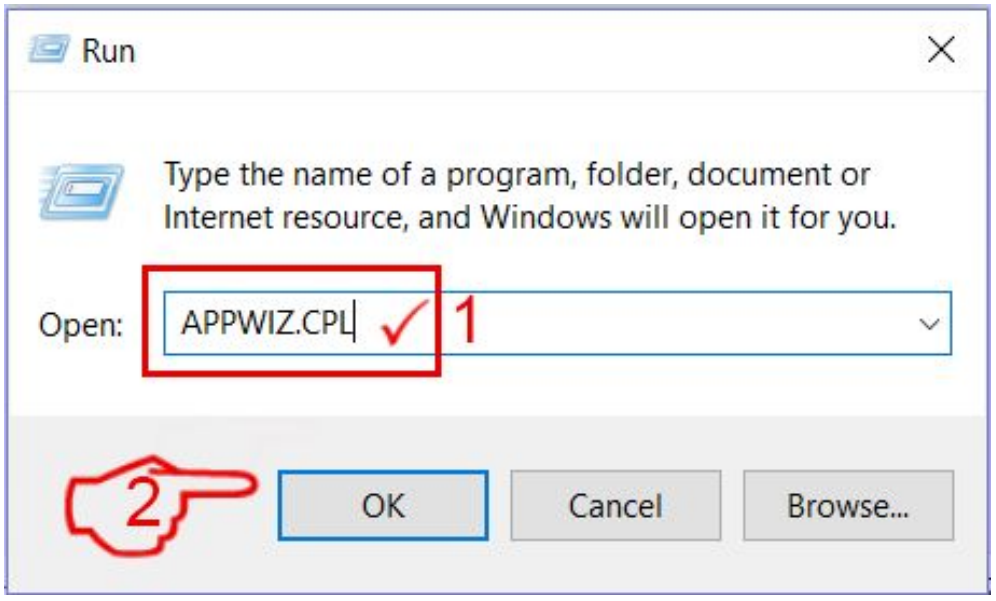
Here is a method in few easy steps that should be able to uninstall most programs. No matter if you are using Windows 10, 8, 7, Vista or XP, those steps will get the job done. Dragging the program or its folder to the recycle bin can be a **very bad decision**. If you do that, bits and pieces of the 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.

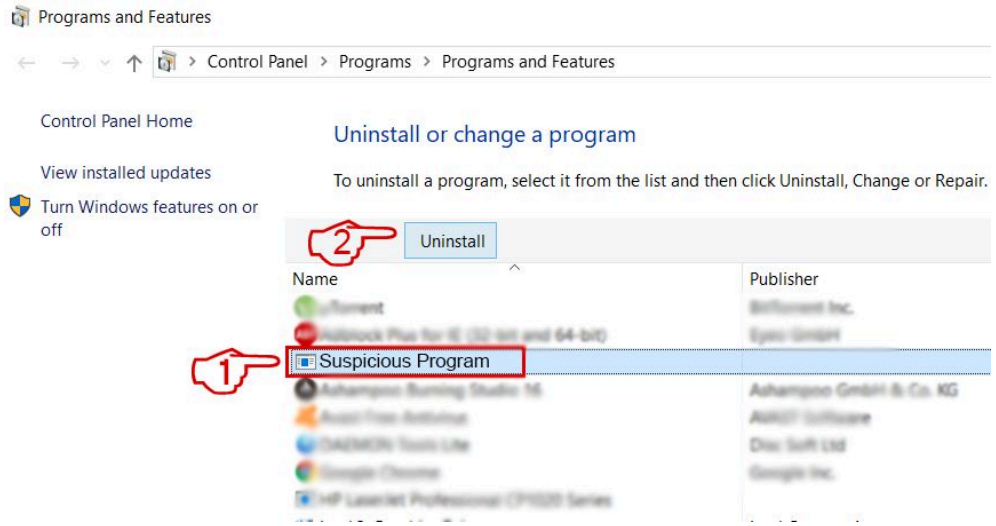
---

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 delete most unwanted and malicious programs.

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

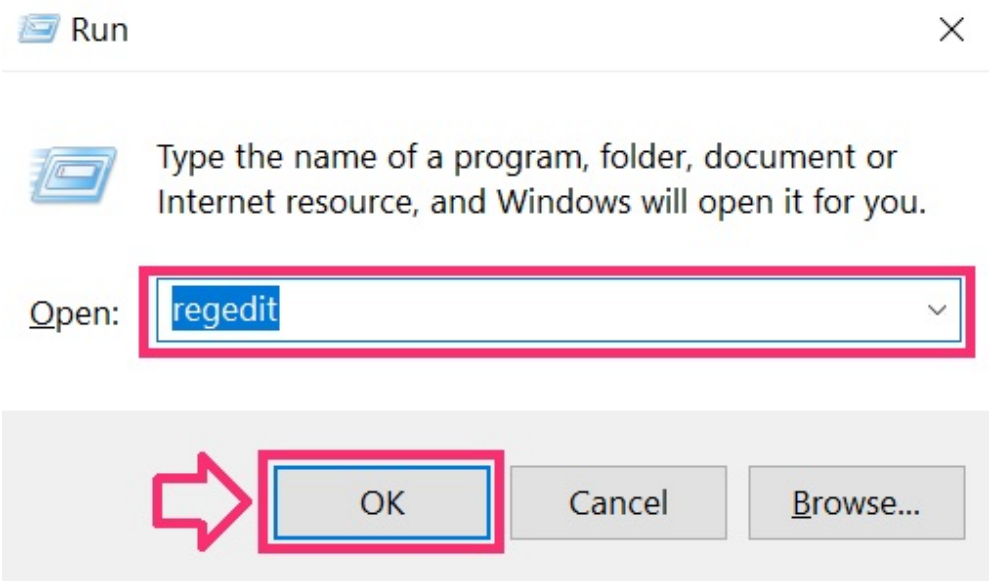
The usually targeted registries of Windows machines are the following:

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

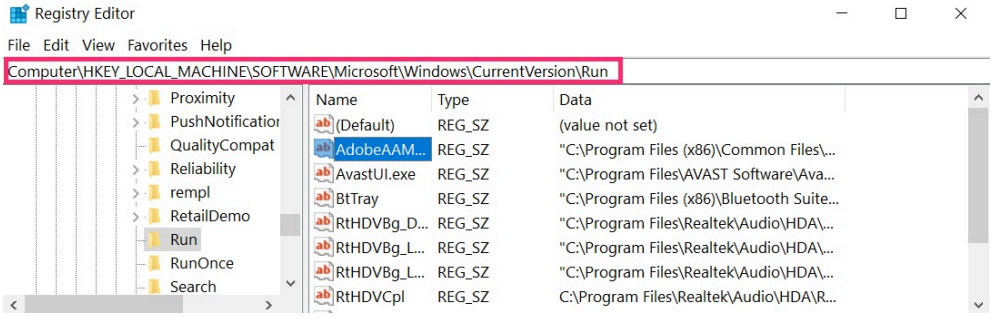
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

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:

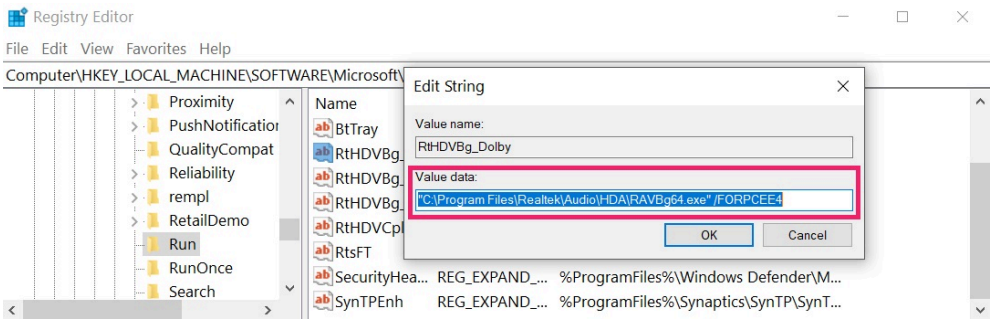
1. Open the **Run Window** again, type **"regedit"** and click OK.



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!

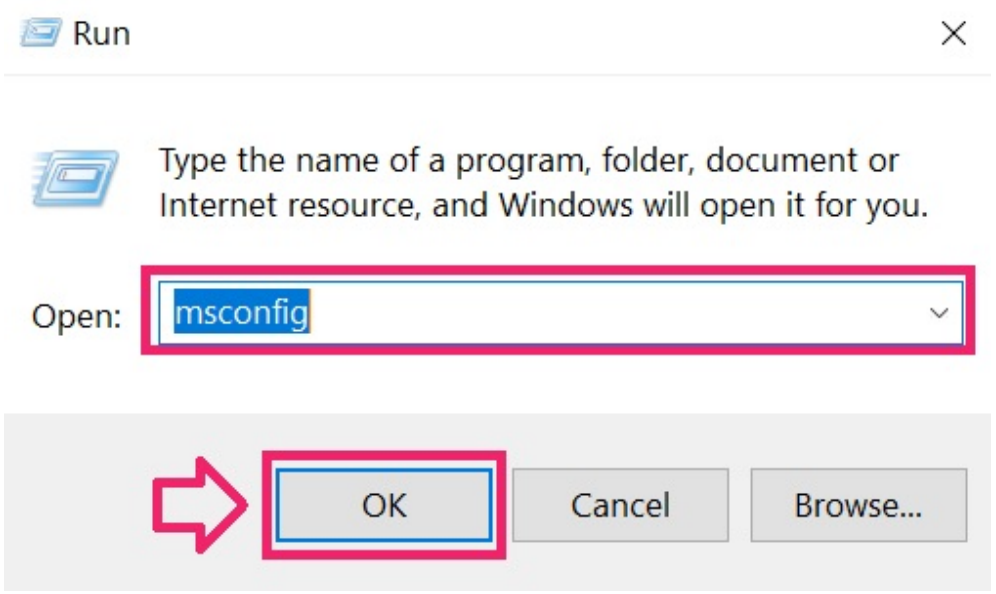
Before starting ***"Step 4"****, please* ***boot back into Normal mode, in case you are currently in Safe Mode****.*

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

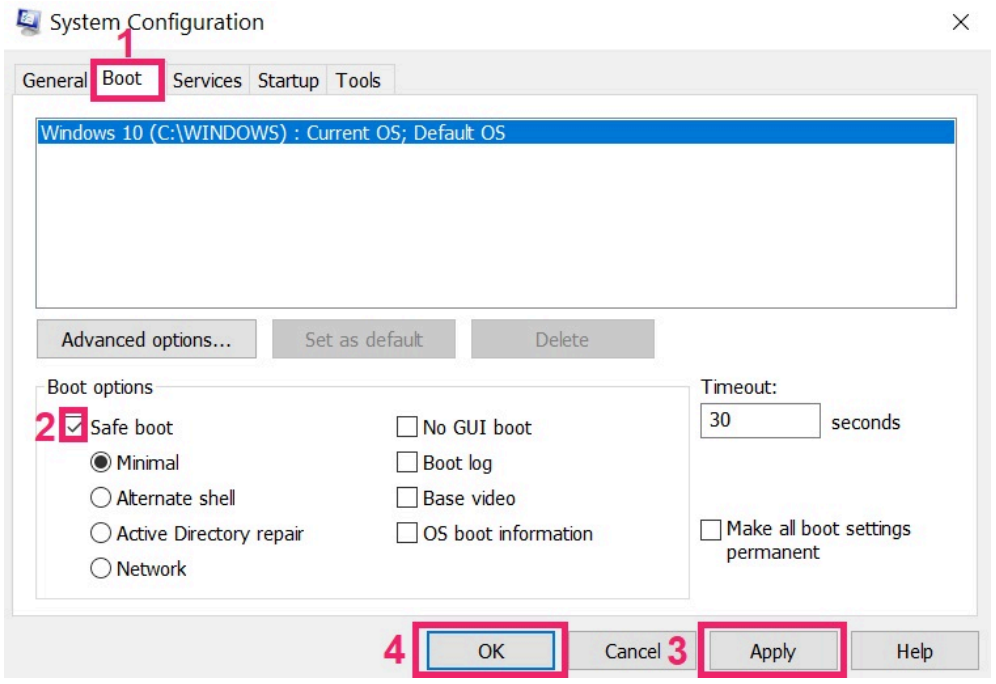
Step 4: Boot Your PC In Safe Mode to isolate and remove .lockymap Ransomware

1. Hold Windows Key + R.

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

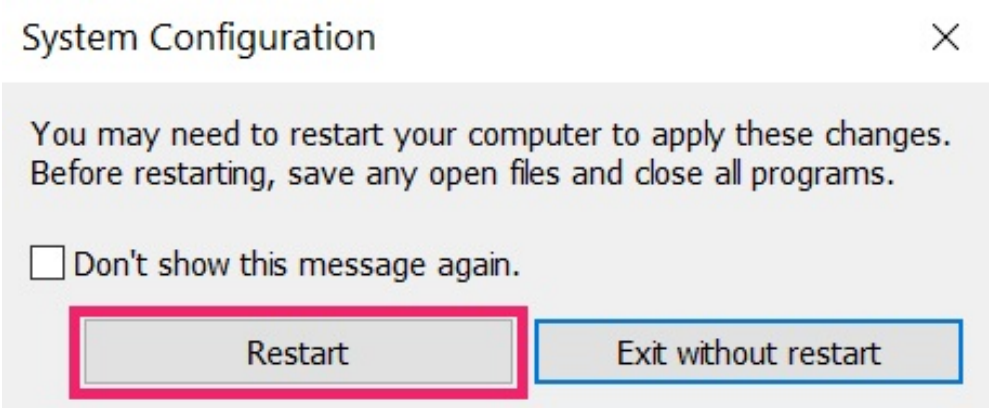


3. Go to the "Boot" tab. There select "Safe Boot" and then click "Apply" and "OK".

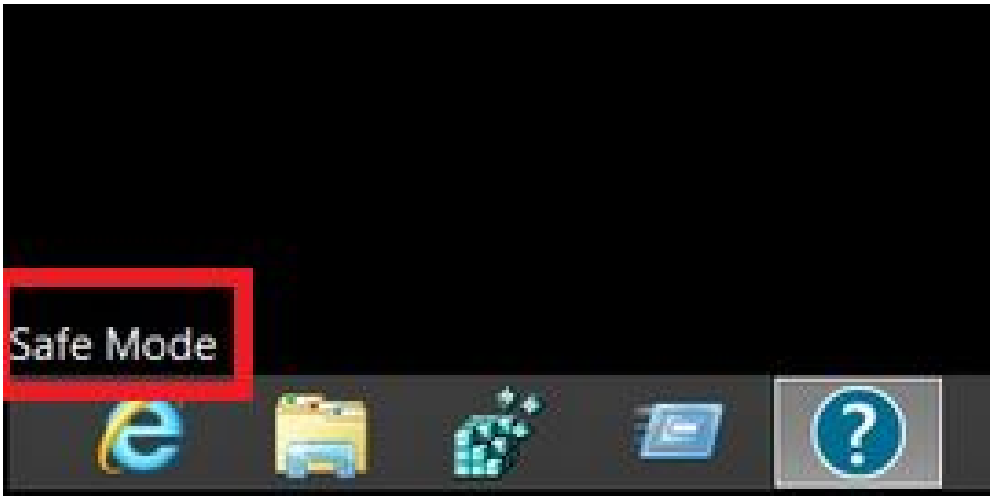


Tip: Make sure to reverse those changes by unticking Safe Boot after that, because your system will always boot in Safe Boot from now on.

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.



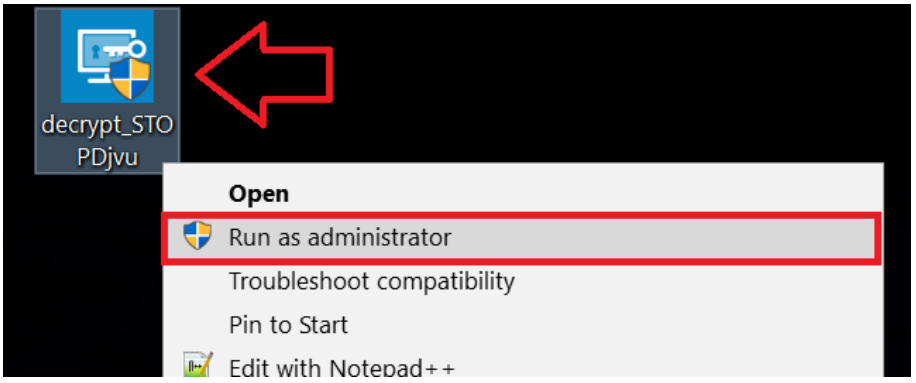
Step 5: Try to Restore Files Encrypted by .lockymap Ransomware.

Method 1: Use STOP Decrypter by Emsisoft.

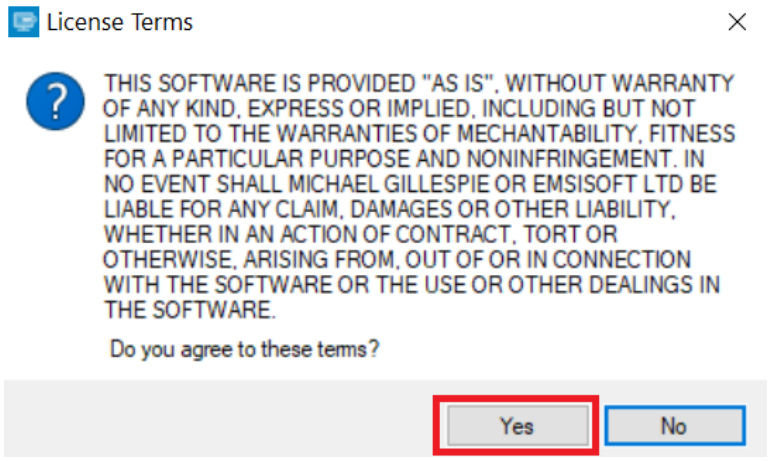
Not all variants of this ransomware can be decrypted for free, but we have added the decryptor used by researchers that is often updated with the variants which become eventually decrypted. You can try and decrypt your files using the instructions below, but if they do not work, then unfortunately your variant of the ransomware virus is not decryptable.

Follow the instructions below to use the Emsisoft decrypter and decrypt your files for free. You can download the Emsisoft decryption tool linked here and then follow the steps provided below:

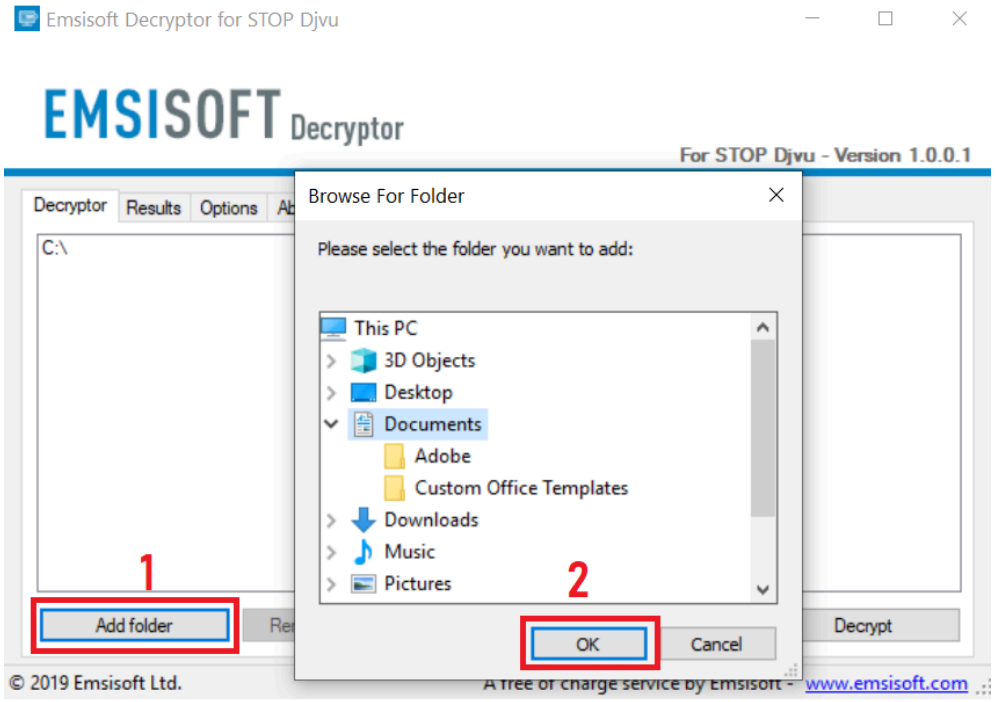
1 Right-click on the decrypter and click on **Run as Administrator** as shown below:



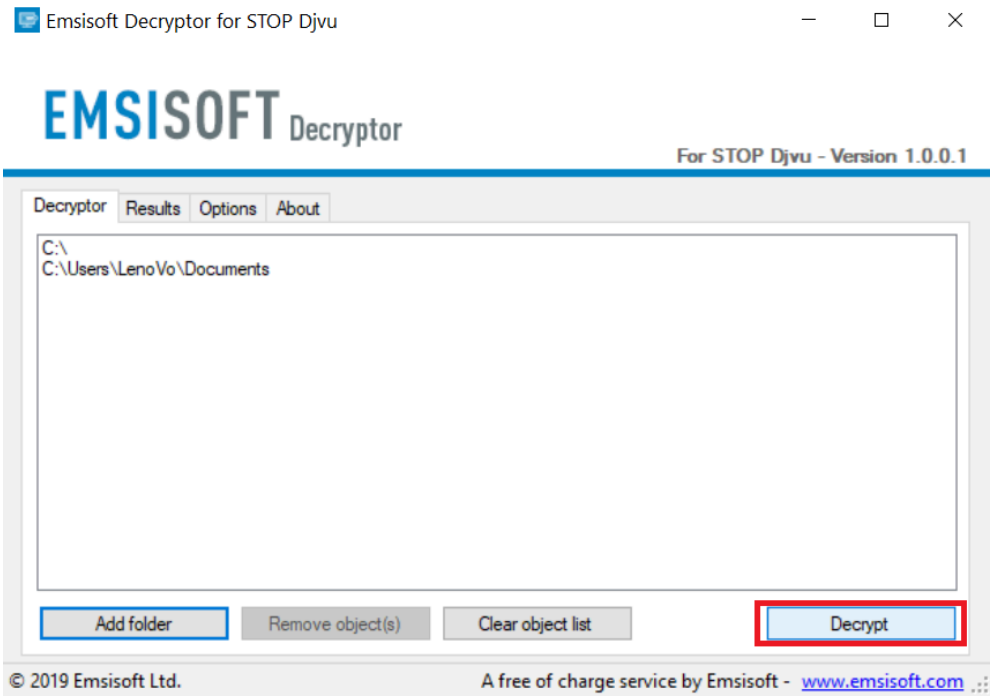
2. Agree with the license terms:



3. Click on "**Add Folder**" and then add the folders where you want files decrypted as shown underneath:



4. Click on "Decrypt" and wait for your files to be decoded.



Note: Credit for the decryptor goes to Emsisoft researchers who have made the breakthrough with this virus.

Method 2: Use data recovery software

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 recommended Data Recovery software by clicking on the link underneath:

Simply click on the link and on the website menus on the 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?

.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 algorithms 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.

What Does .lockymap Ransomware Ransomware Do?

Ransomware in general is a malicious software that is designed **to block access to your computer or files** until a ransom is paid.

Ransomware viruses can also **damage your system**, corrupt data and delete files, resulting in the permanent loss of important files.

How Does .lockymap Ransomware Infect?

Via several ways..lockymap Ransomware Ransomware infects computers by being sent **via phishing emails, 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.

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** without a decryptor. At this point, the **..lockymap Ransomware** files are **encrypted**. You can only open them once they are decrypted using a specific decryption key for the particular algorithm.

What to Do If a Decryptor Does Not Work?

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

Can I Restore "..lockymap Ransomware" Files?

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% guaranteed that you will be able to get your files back. But if you have a backup, your chances of success are much greater.

How To Get Rid of .lockymap Ransomware Virus?

The safest way and the most efficient one for the removal of this ransomware infection is the use a **professional anti-malware program**.

It will scan for and locate .lockymap Ransomware ransomware and then remove it without causing any additional harm to your important ..lockymap Ransomware files.

Can You Stop Ransomware from Encrypting Your Files?

Yes, **you can prevent ransomware**. The best way to do this is to ensure your computer system is updated with the latest security patches, **use a reputable anti-malware program** and firewall, backup your important files frequently, and avoid clicking on malicious links or downloading unknown files.

Can .lockymap Ransomware Ransomware Steal Your Data?

Yes, in most cases ransomware **will steal your information**. It is a form of malware that steals data from a user's computer, encrypts it, and then demands a ransom in order to decrypt it.

In many cases, the malware authors or attackers will threaten to delete the data or publish it online unless the ransom is paid.

Can Ransomware Infect WiFi?

Yes, ransomware can infect WiFi networks, as malicious actors can use it to gain control of the network, steal confidential data, and lock out users. If a ransomware attack is successful, it could lead to a loss of service and/or data, and in some cases, financial losses.

Should I Pay Ransomware?

No, **you should not pay ransomware extortionists**. Paying them only encourages criminals and does not guarantee that the files or data will be restored. The better approach is to have a secure backup of important data and be vigilant about security in the first place.

What Happens If I Don't Pay Ransom?

If you don't pay the ransom, **the hackers may still have access to your computer**, data, or files and may continue to threaten to expose or delete them, or even use them to commit cybercrimes. In some cases, they may even continue to demand additional ransom payments.

Can a Ransomware Attack Be Detected?

Yes, ransomware can be detected. Anti-malware software and other advanced security tools **can detect ransomware and alert the user** when it is present on a machine.

It is important to stay up-to-date on the latest security measures and to keep security software updated to ensure ransomware can be detected and prevented.

Do Ransomware Criminals Get Caught?

Yes, **ransomware criminals do get caught**. Law enforcement agencies, such as the FBI, Interpol and others have been successful in tracking down and prosecuting ransomware criminals in the US and other countries. As ransomware threats continue to increase, so does the enforcement activity.

About the .lockymap Ransomware Research

The content we publish on SensorsTechForum.com, this .lockymap Ransomware how-to removal guide included, is the outcome of extensive research, hard work and our team's devotion to help you remove the specific malware and restore your encrypted files.

How did we conduct the research on this ransomware?

Our research is based on an independent investigation. We are in contact with independent security researchers, and as such, we receive daily updates on the latest malware and ransomware definitions.

Furthermore, the research behind the .lockymap Ransomware ransomware threat is backed with VirusTotal and the NoMoreRansom project.

To better understand the ransomware threat, please refer to the following articles which provide knowledgeable details.

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.
- Verify Facebook, LinkedIn and Twitter personal profiles.

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: