.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.

Finance the adviced: Name information is not least. But Bronymind. Is order for you is not nearly and Mills you have to morthous Bergster. Ballas this stage to restrue your Villes. I' doubland the bir bronsers, () Art type is goingts "doubland You"). I' doubland the bir bronsers, () Art type is goingts "doubland You"). I' doubland the bir bronsers, () Art type is goingts "doubland You"). I' doubland the bir bronsers, () Art type is goingts "doubland You"). I' bronses to the it type is goingt the restrue your files, then you can restore 1 file of image format for free, We are using 3D is a RECOMMENDED. I's using the time is type is goingt that the doubled enery We have to use it within. We are using 3D is a RECOMMENDED. GainTable Canadian on out ty to modify or dolkte may userystaf file as it will be hard to restore 1t. Second to not try to modify our dolkte may userystaf file as it will be hard to restore 1t. Second is they have black to have black down your compared files the you. Canadian and support to have black may accepted files the you.

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
Туре	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 <u>Download</u> <u>Malware Removal Tool</u>
User Experience	Join Our Forum to Discuss .lockymap Ransomware.
Data Recovery Tool	<u>Windows Data Recovery by Stellar Phoenix</u> 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:

From Ozean <brenda.hodges@bxgcorp.com> 🏠</brenda.hodges@bxgcorp.com>	🆘 Reply	🆇 Reply All	▼ 🕈 Forward
Subject News about your order2105586505244		Date Tue,	10 Oct 2017 1
Reply to Ozean <anjali@xcelcorp.com> 🏠</anjali@xcelcorp.com>			
To [removed] <> 🛱			

News about your orderHello Client,

Your order 5122YF5EB72541, placed on 05-10-2017, has just been sent. The Credit Card used for this purchase has been charged today for the total amount of USD 415,70. Your order has been shipped with UPS and has been assigned the following Tracking Number: 97628729. Please allow a few hours for the tracking information to be updated on the site. For more information, see the attached file

The delivery of your order could be delayed due to Customs processing. You can check the delivery status directly in the section Track your order in the Customer Care area.

2017-10-10 Ozean

Ξ	I attachment: Copy document.doc 262 KB	+
	Copy document.doc 262 KB	

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 of 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:

E

Previous post

<u>Next post</u>

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 <u>EULA</u> and <u>Privacy Policy</u>*

- 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 <u>our SpyHunter 5 review</u>. Click on the corresponding links to check SpyHunter's <u>EULA</u>, <u>Privacy Policy</u> and <u>Threat Assessment Criteria</u>

1. Hold Windows key(*) + R

Esc	~ 、	!	1	@ 2	# 3	\$ _	% 1	5	6 8	7	8	9	0 -	- +	=		Home	PgUp	Nav
Tab	Q		W	E	R	Т		Y	U	I	0	Р	{ [}]	E	nter	End	PgDn	Mv Up
Caps	,	Ą	S	C)	F	G	н	J	К	L			\			Insert	Pause	Mv Dn
Shift			Z	Х	C		V	В	Ν	М			?	^	Shift	Del	PrtScn	ScrLk	
Fn	Ctrl			Alt							AltGr	Ctrl	<	$\overline{}$	>		Options	Help	Fade

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

🗁 Run

Х



Type the name of a program, folder, document or Internet resource, and Windows will open it for you.



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

System Configuration								
General Boot Services Startu	ip Tools							
Windows 10 (C:\WINDOWS) :	Current OS; Default OS							
Advanced options	Set as default Delete							
Boot options		Timeout:						
2 🔽 Safe boot	No GUI boot	30 seconds						
Minimal	Boot log							
◯ Alternate shell	Base video							
O Active Directory repair	OS boot information	Make all boot settings						
○ Network		permanent						
		Apply						
		Арру Нер						

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.

System Configuration						
You may need to restart your computer to apply these changes. Before restarting, save any open files and close all programs.						
Don't show this message again.						
Restart	Exit without restart					

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. <u>To do that:</u>



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.

/ Run		×
	Type the name of a program, folder, document or Internet resource, and Windows will open it for you.	
Open:	APPWIZ.CPL 🖌 1	~
5	OK Cancel Browse	

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**"

à	Programs and Features						
~	\rightarrow \checkmark \uparrow $\overline{\mathfrak{g}}$ > Control	Panel > Programs > Programs and Features					
	Control Panel Home	Uninstall or change a program					
	View installed updates To uninstall a program select it from the list and then click Uninstall Change or i						
Turn Windows features on or off Uninstall							
		Name	Publisher				
		C ulterent (Beflamment Inc.				
		Autolock Plus for IE (32 SH and 64-bit)	Cyana General				
		Suspicious Program					
		Ashampere Burning Studie 16	Ashampoo GmbH & Co. KG				
		Acat Transferration	Autor School &				
		CAENCR Tools Like	Diss: Soft Ltd				
		Cough Churne	Gauge inc.				
		 MP Lastriet Professional (21152) Series 	a a 200 1.51				

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.

📑 Registry Editor	-	- 🗆 X
File Edit View Favorites Help		
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\	Edit String	
> Proximity ^ Name	Edit Stillig /	^
> PushNotification	Value name:	
	RtHDVBg_Dolby	
> Reliability	Value data:	
> rempl	"C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe" /FORPCEE4	
> RetailDemo		
Run ab RtsFT	OK Cancel	
	a REG EXPAND %ProgramEiles%\Windows Defender\M	_
	DEC EVDAND %ProgramEiloc%\Synaptics\SynTD\SynT	
< > Syntreinin	REG_EARAND //rrogrammes//synaptics/syntrysynt	~

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. <u>Download</u>

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 <u>EULA</u>, <u>Privacy Policy</u> and <u>Threat Assessment</u> <u>Criteria</u>.

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'**.

SpyHunter°5			REGISTER!	- C X V: 5.0.30.51 DB: 2018.06.24x01
Home Malware/PC Scan System Guard	HelpDesk Settings			(?) (i) Help About
SpyHunter 5		– 🗆 ×		
Malware/PC Scan Custom Scan Scan History Disabled	d Quarantine Exclusions	(?) Help		
Malware/ Quick S Start Sc	PC Scan can (?)			

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.

🛞 SpyHur	scan 17 s	Complete! ecurity Issues Found		■ 17 / 1458264 REGISTER!	− □ × V: 5.0.30.51 DB: 2018.06.24x01
Home Active Scal	Malware/PC Scan	System Guard HelpDesk	န်ဝို့ Settings		(?) Help About
🗹 🛱 Malware: 3	🗌 💿 Privacy: 14	A Whitelisted: 721			
Below is a list of generally repre removed. Shou	malware objects detecte sents a security threat an Id you wish not to remov	d on your computer. Malware ma d should be removed from your s re any of these objects, you may	ay include spyware, adware, troj system as soon as possible. Eacl uncheck them below.	ans, ransomware, worms, viruses, and n of the objects identified below has be	rootkits. Malware en pre-set to be
- ✓ ∅ Safewebse your settin + ✓ □ [F] Production	S arches.com uses misleadin gs to their servers, and m eferences	afewebsearches.com (1 ob ng practices to hijack your brows ay intercept and track your web	ject) er, search results, and other Inte searches and other data.	ernet settings. Once installed, Safewebs	searches.com may lock
PriceChop web brows screensave advertisem words, you may have	A s an adware program tha er, toolbar or within an ac rs. PriceChop may track ents to you or for other a are not personally identi some side effects like slow	dware.PriceChop (1 object) at can automatically display or doo I-supported program. Adware oft your Web browsing habits, sites v advertising and marketing purpos field during the collection of the init computer performance and ann) wnload advertisements to a con en comes bundled with freewar visited, ad usage information, an es. In addition, the data collecte formation. Although PriceChop i oying pop-up ads.	puter. These advertisements may app e such as games, emoticons, file-sharin d transmit that data to third parties to d by adware like PriceChop is generally may not pose a serious threat to your	ear in a pop-up window, g software, or deliver targeted r non-identifiable; in other privacy or security, it
+ • [F] wr	c@avast.com.xpi				
- V I Amagement	Foolbar resets your brow that it is exposed to varie	lindspark Toolbars (1 object ser homepage and adds a new se bus security issues and should be	t) arch engine that may collect da regarded as insecure.	ta about you. Mindspark Toolbar state	s in its own user
				Nex	ct 🖸

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: <u>EaseUS Data Recovery Software</u>

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 <u>EULA</u> and <u>Privacy Policy</u>

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

Ű.	Finder	File	Edit	View	Go	Window	Help	
-		•	<	7	Ba For En	ck rward closing Fok All My Files	der s	೫[೫] ೫↑ ℃೫F
		Fa () (vorites All I Ar App Des Doc Dov	My Files blication: ktop cuments vnloads		Documents Desktop Downloads Home Computer Network iCloud Driv Application	5 5 70 15	 か器O
			wices MA VM	C OS X ware Too	Re Go Co	cent Folder to Folder nnect to Se	rs ərver	ひまU ▶ ひ業G 業K

2. Find Activity Monitor and double-click it:



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

Activity Monitor (My Processes)							
0 0 * -	CPU M	emory Energy	Disk	Network			Q Search
Process Name	Memory ~	Compressed M	Threads	Ports	PID	User	
Photoshop 00	3.23 08	3.15 GB	47	531	38560	Мах	
· Boogie Divorse Herper	2.74.08	2.22.08	19	208	42601	Max	
Y Sketch	2.46.08	1.82.08	40	390	47858	Max	
Adobe Hustrator CC 2015	1.46.08	1.35.08	32	509	41915	Max	
C Statis	1.23.08	558.8 MB	29	504	915	Мак	
Google Chrome Heiper	879.3 MB	578.9 MB	22	190	42603	Мах	
💟 Virus App	751.8 MB	692.7 MB	13	453	981	Max	
Google Chrome	486.1 MB	274.4 MB	44	875	42583	Max	
Constant Constant Margar	460.3 MB	414.5 MB	12	1.00		Max.	
Creative Disust	458.0 MB	428.1 MB	33	1,363	17240	Max	
Monosmap	435.1 MB	354.7 MB	14	334	697	Max	
A Spottly response	402.8 MB	275.8 148	14	121	10824	Max	
 Finalize 	427.9 MB	277.1 48	10	875	12085	Max.	
Adute Destroy Bervice	407.1 MB	366.3 168		1.16	18908	Max	
Admine PEE Mainer	406.8 MB	372.6.MB		134	17254	Max	

Tip: To quit a process completely, choose the "Force Quit" option.

000	_	Activity Mon	itor			
	1 (3)	Other User P	Other User Processes Q*			
Quit Process	Inspect Sample Proce	55	Show		File	ter
PID Pro	cess	1000			No. of Concession, Name	Kind
181	1	Are you sure you wan	t to quit this	process?	18	Intel (64 bit)
8631	1			1000000000	18	intel (64 bit)
0020					28	Intel (64 bit)
104		1.000			(8	Intel (64 (61)
100.00		Force Quit	Cancel	Ouit	18	Intel (64 (60)
1.0		roice Quit	Cancer	Quit	18	Intel (64 (60)
8413	UNDITURD	_usomuxu	0.0	,	Bhross	Intel (64 (60)
239	consulted	_coreaudiod	0.0	3	3.9 MB	Intel (64 (nt)
8583	lecational	Jocationd	8.0	7	3.2 MB	Intel (64 bit)

4. Click on the **"Go"** button again, but this time select **Applications**. Another way is with the **î+∄**+**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**".

Favorites	A	Z	3441E (ST	JUL
Anthony				
Applications				17
		100	111	
Desktop A	pp Store	Automator	Calculator	Calendar
Documents				
O Downloads	1		0	@ 7 0
Movies				
🞵 Music Sur	spicious App	Coca	Contacts	Dashboard
i Pictures				
Dropbox		Directorers	••	DYD
MirDrop	TO:	Aa		(
Devices	Deliveries	Dictionary	Dropbox	DVD Player

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 \(\mathcal{H}+A\) 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:

📫 Fine	der File	Edit	View	Go	Window	Help				C	
1	1			Ba Fo Se	ick rward lect Startu	p Disk on	Desktop	೫[೫] ৫೫↑	4	2	
					Recents Document Desktop Download Home Library Computer AirDrop Network iCloud Driv Applicatio	s ve ns	Desktop	 か器F 			
1				Re	Utilities cent Folde	rs		ີ ୁ ଜжሀ ►			
		-		Go Co	o to Folder onnect to S	erver		<mark> </mark>			
19/		-		-	- A	K					

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

	Go to Folder	
Go to the folder:		
/Library/LaunchAgents		~
	Cancel	Go

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.

• •	LaunchAgents	
< >		Q Search
Back/Forward Dropbox	View Arrange Action Share	Search
Favorites	Name ~	Date Modified
iCloud	* com.teamviewer.teamviewer.plist	Today at 9:59 AM
leibuu	* com.teamviewer.teamviewer_desktop.plist	Today at 9:59 AM
Devices	🐑 com.oracle.java.Java-Updater.plist	Nov 9, 2015 at 4:42 PM
Shared	Com.microsoft.update.agent.plist	Apr 12, 2018 at 3:47 PM
	Com.google.keystone.agent.plist	Jul 11, 2016 at 9:23 PM
	com.adobe.ARMDCHelpc8e43c37a23d420d.plist	May 8, 2018 at 10:05 PM
White Rabbit		
	📓 Macintosh HD 🔸 🛅 Library 🔸 🛅 LaunchAgents	
×	6 items, 32.3 GB available	

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

 \rightarrow ~/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

Scanning Files: 19% C:\Program Files\Adobe\Adobe Photoshop CS6 (x64)\Lega\\fr_MA\\icense.html 16 / 1312020 STOP	- □ × V: 5.0.30.51 DB: 2018.06.24×01
Home Active Scan Malware/PC Scan System Guard HelpDesk Settings	(?) (i) Help About
✓ ∰ Malware: 2	
Below is a list of malware objects detected on your computer. Malware may include spyware, adware, trojans, ransomware, worms, virus generally represents a security threat and should be removed from your system as soon as possible. Each of the objects identified below removed. Should you wish not to remove any of these objects, you may uncheck them below.	es, and rootkits. Malware r has been pre-set to be
Safewebsearches.com (1 object) Safewebsearches.com uses misleading practices to hijack your browser, search results, and other Internet settings. Once installed, Sa your settings to their servers, and may intercept and track your web searches and other data.	afewebsearches.com may lock
 ✓ I Adware.PriceChop (1 object) PriceChop is an adware program that can automatically display or download advertisements to a computer. These advertisements m web browser, toolbar or within an ad-supported program. Adware often comes bundled with freeware such as games, emoticons, file PriceChop may track your Web browsing habits, sites visited, ad usage information, and transmit that data to third parties to deliver for other advertising and marketing purposes. In addition, the data collected by adware like PriceChop is generally non-identifiable; in personally identified during the collection of the information. Although PriceChop may not pose a serious threat to your privacy or see effects like slow computer performance and annoying pop-up ads. + ✓ C [F] wrc@avast.com.xpi 	nay appear in a pop-up window, e-sharing software, or screensavers. targeted advertisements to you or other words, you are not ecurity, it may have some side
Please wait for the SpyHunter scan to complete	anning 🖏

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: <u>EaseUS Data Recovery Software</u>

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 <u>ransomware</u> 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 <u>encrypted</u>. You can only open them once they are decrypted.

Decryptor did not decrypt my data. What now?

Do not panic and **<u>backup the files</u>**. 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 <u>decryptor</u> 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 redownload 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 <u>forums</u>, 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 <u>cybercrime</u>:

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

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

- 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.