CryptoLocker Ransomware Information Guide and FAQ

Cem Öztürk

….on October 14, 2013 @ 03:09 PM | Last Updated: October 31, 2014 |

Info: The original CryptoLocker infection was disabled on June 2nd, 2014 when Operation Gameover took down its distribution network. Since then there have been numerous ransomware infections that have been released that utilize the CryptoLocker name. It should be noted that these infections are not the same infection that is discussed below. If you have recently been infected with something that is calling itself CryptoLocker, you are most likely infected with the TorrentLocker infection. For more information on TorrentLocker, please visit our TorrentLocker support topic. Once at the topic, and if you are a member, you can subscribe to it in order to get notifications when someone adds more information to the topic.

Table of Contents

The purpose of this guide

There is a lot of incorrect and dangerous information floating around about CryptoLocker. As BleepingComputer.com was one of the first support sites to try helping users who are infected with this infection, I thought it would be better to post all the known information about this infection in one place. This FAQ will give you all the information you need to understand the infection and restore your files via the decrypter or other methods.

In many ways this guide feels like a support topic on how to pay the ransom, which sickens me. Unfortunately, this infection is devious and many people have no choice but to pay the ransom in order to get their files back. I apologize in advance if this is seen as helping the developers, when in fact my goal is to help the infected users with whatever they decide to do.

All of this information has been compiled from my own experimentation with this infection, from Fabian Wosar of **Emsisoft** who first analyzed this infection, and through all the consultants and visitors who contributed to our 207 page **CryptoLocker support topic**. Big thanks to everyone who contributed information about this infection. This guide will continue to be updated as new information or approaches are gathered. If you have anything that you think should be added, clarified, or revised please let us know in the support topic linked to above.

Info: There is a very active CryptoLocker support topic, which contains discussion and the experiences of a variety of IT consultants, end users, and companies who have been affected by CryptoLocker. If you are interested in this infection or wish to ask questions

about it, please visit this CryptoLocker support topic. Once at the topic, and if you are a member, you can subscribe to it in order to get notifications when someone adds more information to the topic.

What is CryptoLocker

CryptoLocker is a ransomware program that was released around the beginning of September 2013 that targets all versions of Windows including Windows XP, Windows Vista, Windows 7, and Windows 8. This ransomware will encrypt certain files using a mixture of RSA & AES encryption. When it has finished encrypting your files, it will display a CryptoLocker payment program that prompts you to send a ransom of either $100 or $300 in order to decrypt the files. This screen will also display a timer stating that you have 72 hours, or 4 days, to pay the ransom or it will delete your encryption key and you will not have any way to decrypt your files. This ransom must be paid using MoneyPak vouchers or Bitcoins. Once you send the payment and it is verified, the program will decrypt the files that it encrypted.

CryptoLocker payment screen
For more screen shots of this infection click on the image above.
There are a total of 3 images you can view.

When you first become infected with CryptoLocker, it will save itself as a random named filename to the root of the %AppData% or %LocalAppData% path. It will then create one of the following autostart entries in the registry to start CryptoLocker when you login:

```
KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "CryptoLocker"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce "*CryptoLocker"
KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "CryptoLocker_<version_number>"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce "*CryptoLocker_<version_number"
```

Please note that the * in front of the RunOnce value causes CryptoLocker to start in Safe Mode.

The infection will also hijack your .EXE extensions so that when you launch an executable it will attempt to delete the Shadow Volume Copies that are on the affected computer. It does this because you can use shadow volume copies to restore your encrypted files. The command that is run when you click on an executable is:

"C:\Windows\SYsWOW64\cmd.exe" /C "C:\Windows\Sysnative\vssadmin.exe" Delete Shadows /All /Quiet

The .EXE hijack in the Registry will look similar to the following. Please note that registry key names will be random.

```
[HKEY_CLASSES_ROOT\.exe]
@="Myjiaabodehhltdr"
"Content Type"="application/x-msdownload"

[HKEY_CLASSES_ROOT\.exe\PersistentHandler]
@="{098f2470-bae0-11cd-b579-08002b30bfeb}"

[HKEY_CLASSES_ROOT\Myjiaabodehhltdr]

[HKEY_CLASSES_ROOT\Myjiaabodehhltdr\DefaultIcon]
@="%1"

[HKEY_CLASSES_ROOT\Myjiaabodehhltdr\shell]
```

```
[HKEY_CLASSES_ROOT\Myjiaabodehhltdr\shell\open]

[HKEY_CLASSES_ROOT\Myjiaabodehhltdr\shell\open\command]
@="\"C:\\Users\\User\\AppData\\Local\\Rlatviomorjzlefba.exe\" - \"%1\" %*"
```

Once the infection has successfully deleted your shadow volume copies, it will restore your exe extensions back to the Windows defaults.

The infection will then attempt to find a live Command & Control server by connecting to domains generated by a **Domain Generation Algorithm**. Some examples of domain names that the DGA will generate are lcxgidtthdjje.org, kdavymybmdrew.biz, dhlfdoukwrhjc.co.uk, and xodeaxjmnxvpv.ru. Once a live C&C server is discovered it will communicate with it and receive a public encryption key that will be used to encrypt your data files. It will then store this key along with other information in values under the registry key under **HKEY_CURRENT_USER\Software\CryptoLocker_0388**. Unfortunately, the private key that is used to decrypt the infected files is not saved on the computer but rather the Command & Control server.

CryptoLocker will then begin to scan all physical or mapped network drives on your computer for files with the following extensions: *.odt, *.ods, *.odp, *.odm, *.odc, *.odb, *.doc, *.docx, *.docm, *.wps, *.xls, *.xlsx, *.xlsm, *.xlsb, *.xlk, *.ppt, *.pptx, *.pptm, *.mdb, *.accdb, *.pst, *.dwg, *.dxf, *.dxg, *.wpd, *.rtf, *.wb2, *.mdf, *.dbf, *.psd, *.pdd, *.pdf, *.eps, *.ai, *.indd, *.cdr, *.jpg, *.jpe, *.jpg, *.dng, *.3fr, *.arw, *.srf, *.sr2, *.bay, *.crw, *.cr2, *.dcr, *.kdc, *.erf, *.mef, *.mrw, *.nef, *.nrw, *.orf, *.raf, *.raw, *.rwl, *.rw2, *.r3d, *.ptx, *.pef, *.srw, *.x3f, *.der, *.cer, *.crt, *.pem, *.pfx, *.p12, *.p7b, *.p7c. When it finds files that match one of these types, it will encrypt the file using the public encryption key and add the full path to the file and the filename as a value under the **HKEY_CURRENT_USER\Software\CryptoLocker_0388\Files** Registry key.

When it has finished encrypting your data files it will then show the CryptoLocker screen as shown above and demand a ransom of either $100 or $300 dollars in order to decrypt your files. This ransom must be paid using Bitcoin or MoneyPak vouchers. It also states that you must pay this ransom within 96 hours or the private encryption key will be destroyed on the developer's servers.

Warning: If you enter an incorrect payment code, it will decrease the amount of time you have available to decrypt your files. So if you plan on paying the ransom, please be careful as you type the code.

More technical details about this infection can be at this **blog post** by Emsisoft.

Known file paths and registry keys used by CryptoLocker

This section lists all known file paths and registry keys used by CryptoLocker. The file paths and registry keys that are currently being used by CryptoLocker will be highlighted in **blue.**

The File paths that are currently and historically being used by CryptoLocker are:

%AppData%\<random.exe> and **%AppData%\{<8 chars>-<4 chars>-<4 chars>-<4 chars>-<12 chars>}.exe**

Examples of filenames using this path are: **Rlatviomorjzlefba.exe** and **{34285B07-372F-121D-311F-030FAAD0CEF3}.exe**.

In Windows XP, %AppData% corresponds to C:\Documents and Settings\<Login Name>\Application Data.
In Windows Vista, 7, and 8, %AppData% corresponds to C:\Users\<Login Name>\AppData\Roaming.

%LocalAppData%\<random.exe>

Examples of filenames using this path are: **Rlatviomorjzlefba.exe**.

In Windows XP, %LocalAppData% corresponds to C:\Documents and Settings\<Login Name>\Local Settings\Application Data\.
In Windows Vista, 7, and 8, %LocalAppData% corresponds to C:\Users\<Login Name>\AppData\Local.

The Registry key that is used to automatically start CryptoLocker when you login to Windows are found below.

KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "CryptoLocker_<version_number>"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce "*CryptoLocker_<version_number"

For the above registry values, the current version is **0388**. Please note that the ***** in the RunOnce entry tells Windows to start CryptoLocker even in Windows Safe Mode.

CryptoLocker also creates a registry key to store its configuration information and the files that were encrypted. In the past the registry key that was used was HKEY_CURRENT_USER\Software\CryptoLocker. Newer version now include the version of the malware, which is currently 0388, in the key name.

The registry key that is currently being used to store the configuration information is **HKEY_CURRENT_USER\Software\CryptoLocker_0388**. Under this key are 3 registry values that are described below:

Value Name	Description
PublicKey	The **PublicKey** value contains the public key that was used to encrypt your files. This key will not help you decrypt the encrypted files on your computer.
VersionInfo	The **VersionInfo** value contains information that includes the current version of the malware, the IP address of the Command & Control server, and the timestamp of installation.
Wallpaper	The **WallPaper** value contains information regarding the wallpaper that will be shown as the background on the infected computer's desktop.

Under the **HKEY_CURRENT_USER\Software\CryptoLocker_0388\Files** key will be a list of all the files that have been encrypted by CryptoLocker. This list is then processed by the decryption tool to decrypt your files if you paid the ransom. For each file that is encrypted, a new REG_DWORD value will be created that is named using the full pathname to the encrypted file. When naming the values, CryptoLocker will replace all occurrences of the forward slash character (****), with a question mark. An example of how an encrypted file's value entry would be named is **C:?Users?Public?Pictures?Sample Pictures?Penguins.jpg**. You can use the **ListCrilock** program to export a human readable list of these encrypted files from the registry into a text file.

Since the release of **the CryptoLocker Decryption Service** it is possible to decrypt files without this registry key being available. The new decrypter provided by this service will instead scan your files and attempt to decrypt them using the embedded private decryption key.

What should you do when you discover your computer is infected with CryptoLocker

When you discover that a computer is infected with CryptoLocker, the first thing you should do is disconnect it from your wireless or wired network. This will prevent it from further encrypting any files. Some people have reported that once the network connection is disconnected, it will display the CryptoLocker screen.

It is not advised that you remove the infection from the %AppData% folder until you decide if you want to pay the ransom. If you do not need to pay the ransom, simply delete the Registry values and files and the program will not load anymore. You can then restore your data via other methods.

It is important to note that the CryptoLocker infection spawns two processes of itself. If you only terminate one process, the other process will automatically launch the second one again. Instead use a program like **Process Explorer** and right click on the first process and select **Kill Tree**. This will terminate both at the same time.

Is it possible to decrypt files encrypted by CryptoLocker?

Updated 8/6/14:

FireEye and **Fox-IT** have released a method of possibly retrieving your private decryption key and a decrypter to use to decrypt your files. These keys were made available through **Operation Tovar** and were not retrieved by cracking the encryption. To try and retrieve your key, please visit their site**http://www.decryptcryptolocker.com/** and enter your email and upload a copy of one of your CryptoLocker encrypted files. The service will then try attempt to decrypt that file using all of the known encryption keys. If they are able to successfully decrypt your file, they will then email you the decryption key with instructions on how to use it.

In order to use the decryption you need to paste the entire decryption key they send you, quotes and all, after the --key argument of the Decryptolocker.exe program. An example of how you would decrypt all of the folders and files under a particular folder can be found in this **post**. As the instructions and how to use the tool are not particularly user-friendly, if you need any help, please see feel free to ask in the **CryptoLocker Support Topic**. It should also be noted that you can use a different script, that it appears the FireEye/Fox-IT one was based off of, as well. Instructions on using the alternative decrypter can be found **here**.

If your key is not available using the above methods, the only methods you have of restoring your files is from a backup or Shadow Volume Copies if you have System Restore enabled. Newer variants of CryptoLocker attempt to delete the Shadow Copies, but it is not always successful. More information about how to restore your files via Shadow Volume Copies can be found in **this section** below.

If you do not have System Restore enabled on your computer or reliable backups, then you will need to pay the ransom in order to get your files back.

Will paying the ransom actually decrypt your files?

Paying the ransom will start the decryption process of the CryptoLocker infection. When you pay the ransom you will be shown a screen stating that your payment is being verified. Reports from people who have paid this ransom state that this verification process can take 3-4 hours to complete. Once the payment has been verified, the infection will start decrypting your files. Once again, it has been reported that the decryption process can take quite a bit of time.

Be warned, that there have been some reports that the decryption process may give an error stating that it can't decrypt a particular file. At this point we have no information as how to resolve this. Visitors have reported that the infection will continue to decrypt the rest of the files even if it has a problem with certain files.

How do you become infected with CryptoLocker

This infection is typically spread through emails sent to company email addresses that pretend to be customer support related issues from Fedex, UPS, DHS, etc. These emails would contain a zip attachment that when opened would infect the computer. These zip files contain executables that are disguised as PDF files as they have a PDF icon and are typically named something like FORM_101513.exe or FORM_101513.pdf.exe. Since Microsoft does not show extensions by default, they look like normal PDF files and people open them.

When CryptoLocker was first released, it was being distributed by itself. Newer malware attachments appear to be Zbot infections that then install the CryptoLocker infection. You will know you are infected with Zbot as there will be a registry key in the form of:

```
HKCU\Software\Microsoft\<random>
```

Under these keys you will see Value names with data that appears to be garbage data (encrypted info). The droppers will also be found in the %Temp% folder and the main executable will be stored in a random folder under **%AppData%**. Last but not least, a startup will be created under**HKCU\Software\Microsoft\Windows\CurrentVersion\Run** to launch it.

An example Zbot/CryptoLocker email message is:

-----Original Message-----
From: John Doe
[mailto:John@mydomain.com]
Sent: Tuesday, October 15, 2013 10:34 AM
To: Jane Doe
Subject: Annual Form - Authorization to Use Privately Owned Vehicle on State Business

All employees need to have on file this form STD 261 (attached). The original is retained by supervisor and copy goes to Accounting. Accounting need this form to approve mileage reimbursement.

The form can be used for multiple years, however it needs to re-signed annually by employee and supervisor.

Please confirm all employees that may travel using their private car on state business (including training) has a current STD 261 on file. Not having a current copy of this form on file in Accounting may delay a travel reimbursement claim.

The current list of known CryptoLocker email subjects include:

USPS - Your package is available for pickup (Parcel 173145820507)	USPS - Missed package delivery ("USPS Express Services" <service-notification@usps.com>)
USPS - Missed package delivery	FW: Invoice <random number>
ADP payroll: Account Charge Alert	ACH Notification ("ADP Payroll" <*@adp.com>)
ADP Reference #09903824430	Payroll Received by Intuit
Important - attached form	FW: Last Month Remit
McAfee Always On Protection Reactivation	Scanned Image from a Xerox WorkCentre
Scan from a Xerox WorkCentre	scanned from Xerox
Annual Form - Authorization to Use Privately Owned Vehicle on State Business	Fwd: IMG01041_6706015_m.zip
My resume	New Voicemail Message
Voice Message from Unknown (675-685-3476)	Voice Message from Unknown Caller (344-846-4458)
Important - New Outlook Settings	Scan Data
FW: Payment Advice - Advice Ref:[GB293037313703] / ACH credits / Customer Ref:[pay run 14/11/13]	Payment Advice - Advice Ref:[GB2198767]
New contract agreement.	Important Notice - Incoming Money Transfer
Notice of underreported income	Notice of unreported income - Last months reports
Payment Overdue - Please respond	FW: Check copy
Payroll Invoice	USBANK
Corporate eFax message from "random phone #" - 8 pages (random phone # & number of pages)	past due invoices
FW: Case FH74D23GST58NQS	Symantec Endpoint Protection: Important System Update - requires immediate action

Known Bitcoin Payment addresses for CryptoLocker

CryptoLocker allows you to pay the ransom by sending 2 bitcoins to an address shown in the decryption program. Bitcoins are currently worth over $200 USD on some bitcoins exchanges. Earlier variants of CryptoLocker included static bitcoin addresses for everyone who was infected. These static addresses include:

https://blockchain.info/address/18iEz617DoDp8CNQUyyrjCcC7XCGDf5SVb
https://blockchain.info/address/1KP72fBmh3XBRfuJDMn53APaqM6iMRspCh

Newer variants of CryptoLocker dynamically generate new bitcoin payment addresses for each instance of an infection. You can use the links above to see transactions into the wallet and out of the wallet.

CryptoLocker and Network Shares

CryptoLocker only encrypts data stored on network shares if the shared folders are mapped as a drive letter on the infected computer. Despite what some articles state, CryptoLocker **does not** encrypt data on a network through UNC shares. An example of a UNC share is \\computername\openshare.

It is strongly suggested that you secure all open shares by only allowing writable access to the necessary user groups or authenticated users. This is an important security principle that should be used at all times regardless of infections like CryptoLocker.

What to do if your anti-virus software deleted the infection files and you want to pay the ransom!

As many anti-virus programs would delete the CryptoLocker executables after the encryption started, you would be left with encrypted files and no way to decrypt them. Recent versions of CryptoLocker will now set your Windows wallpaper to a message that contains a link to a decryption tool that you can download in case this happens. There are numerous reports that this download will not double-encrypt your files and will allow you to decrypt encrypted files.

How to increase the time you have to pay the ransom

When the CryptoLocker is first shown, you will see a timer that states you need to pay the ransom within 96 hours. Some people have reported that you can increase the time by rolling back the clock in your BIOS. So to increase the timer by 10 hours, you would change your clock in your BIOS to 10 hours earlier. The virus author has **stated** that using this method will not help. They have said that the private key required for decryption will be deleted from the Command & Control server after the allotted time regardless of how much time it says is left on the infected computer.

Tests by users, though, have shown that the private keys are not deleted and you can pay the ransom even if your time has run out. The steps that people have reported to work are:

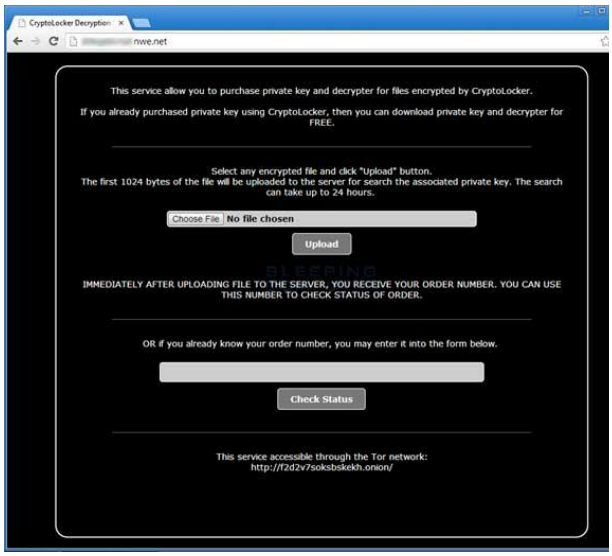
1. Restore CryptoLocker registry key if it was deleted.
2. Immediately shut down computer.
3. Start computer and enter bios. Once in the bios, change your clock to some time in the past to increase the timer.
4. Reboot your computer.
5. CryptoLocker should now show that you have more time left.

It is unknown if this method will still work now that the **CryptoLocker Decryption Service** was created.

Messages from the ransomware author and information about the CryptoLocker Decryption Service

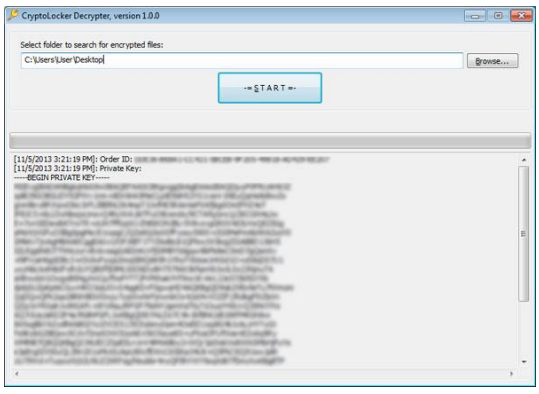
People have asked how they can contact the author of this infection when their payment does not go through. There is no direct way to contact the developer of this computer infection. They are, though, monitoring the various threads about this infection, including our **CryptoLocker support topic**, and have responded to infected user's issues as well as to give other messages on the home page of their Command & Control servers. The address for this Command & Control server can be found on the desktop wallpaper on an infected computer. The url that they specify to download the decrypter, can also be used to view the messages from the author. Simply go to the home page rather than the executable. So if the wallpaper has an URL of http://kjasdklhjlas.info/1002.exe, to see the message you would go to http://kjasdklhjlas.info/. Please note that this url is not valid.

As of 11/01/13, the Command & Control server home page was changed to the CryptoLocker Decryption Service. This decryption service can also be accessed via TOR at the address f2d2v7soksbskekh.onion/. This service allows you to upload an encrypted file that performs a search for your public key. When your public is found if you had previously paid the ransom, it will give you a link to your private key and decrypter. If you had not paid the ransom already then you will be given the option to purchase the private key and a decrypter. The cost of the private key remains 2 bitcoins if you within the standard 72 hour time frame, but if that has expired the price jumps to 10 bitcoins. At 10 bitcoins the ransom payment is over $2,290 USD.



Click on the image above to see full size and other associated images.

Once a payment is made it must have 10-15 bitcoin **confirmations** before your private key and a decrypter will be made available for download. Once these confirmations have occurred a download link will be displayed that will allow you to download a standalone decrypter. This decrypter will already have your private decryption key stored in the program and can be used to scan for and decrypt encrypted files.



Click on the image above to see full size and other associated images.

More information about this decryption service can be found in this news article: **CryptoLocker developers charge 10 bitcoins to use new Decryption Service**.

Previous Command & Control home page messages:

Date	Link to Image
10/22/2013	**http://www.bleepstatic.com/swr-guides/c/cryptolocker/command-control-message-10-22-13.jpg**
10/29/2013	**http://www.bleepstatic.com/swr-guides/c/cryptolocker/command-control-message-10-29-13.jpg**

How to restore files encrypted by CryptoLocker using Shadow Volume Copies

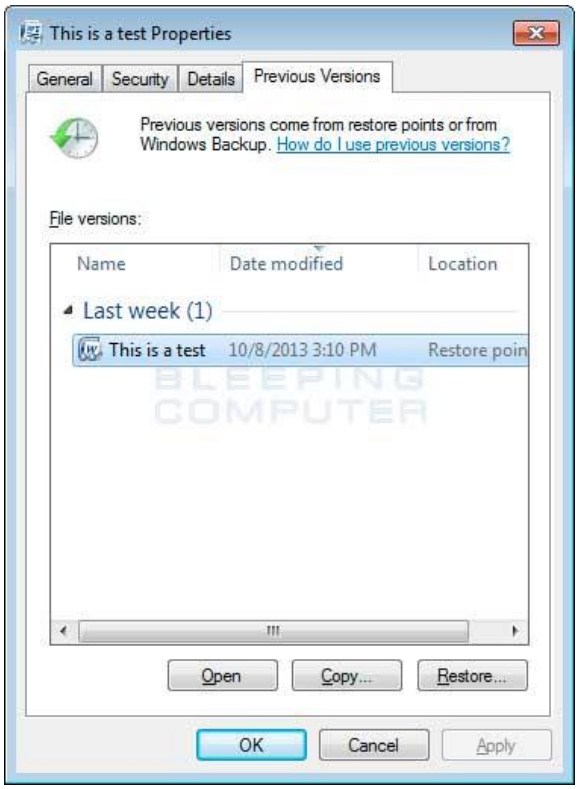
If you had System Restore enabled on the computer, Windows creates **shadow copy snapshots** that contain copies of your files from that point of time when the system restore snapshot was created. These snapshots may allow us to restore a previous version of our files from before they had been encrypted. This method is not fool proof, though, as even though these files may not be encrypted they also may not be the latest version of the file. Please note that Shadow Volume Copies are only available with Windows XP Service Pack 2, Windows Vista, Windows 7, & Windows 8.

Note: Newer variants of CryptoLocker will attempt to delete all shadow copies when you first start any executable on your computer after becoming infected. Thankfully, the infection is not always able to remove the shadow copies, so you should continue to try restoring your files using this method.

In this section we provide two methods that you can use to restore files and folders from the Shadow Volume Copy. The first method is to use native Windows features and the second method is to use a program called Shadow Explorer. It does not hurt to try both and see which methods work better for you.

Using native Windows Previous Versions:

To restore individual files you can right-click on the file, go into **Properties**, and select the **Previous Versions** tab. This tab will list all copies of the file that have been stored in a Shadow Volume Copy and the date they were backed up as shown in the image below.



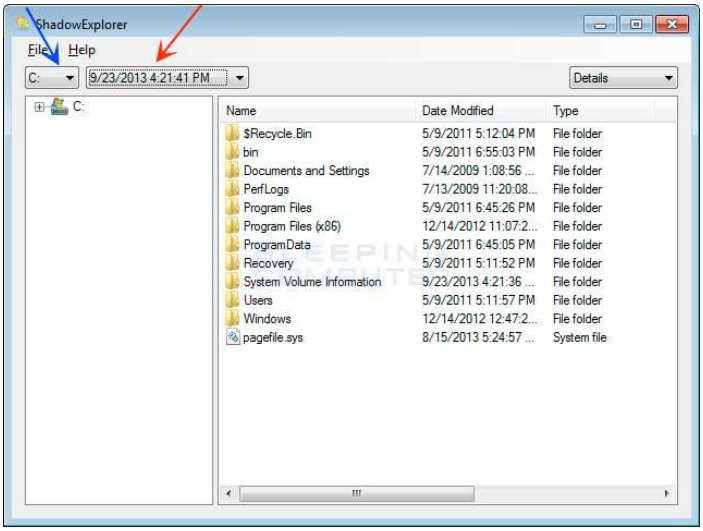
To restore a particular version of the file, simply click on the **Copy** button and then select the directory you wish to restore the file to. If you wish to restore the selected file and replace the existing one, click on the **Restore** button. If you wish to view the contents of the actual file, you can click on the**Open** button to see the contents of the file before you restore it.

This same method can be used to restore an entire folder. Simply right-click on the folder and select **Properties** and then the **Previous Versions** tabs. You will then be presented with a similar screen as above where you can either **Copy** the selected backup of the folder to a new location or **Restore** it over the existing folder.

Using Shadow Explorer:

You can also use a program called **Shadow Explorer** to restore entire folders at once. When downloading the program, you can either use the full install download or the portable version as both perform the same functionality.

When you start the program you will be shown a screen listing all the drives and the dates that a shadow copy was created. Select the drive (blue arrow) and date (red arrow) that you wish to restore from. This is shown in the image below.



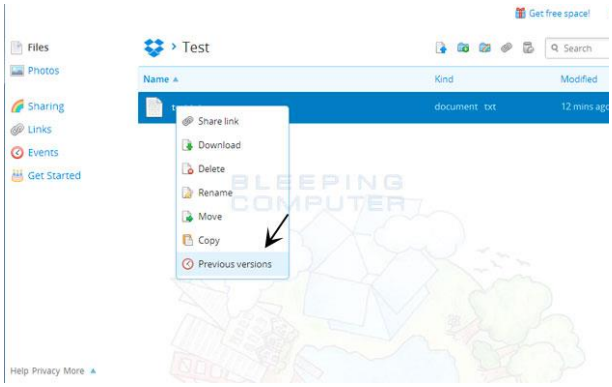
To restore a whole folder, right-click on a folder name and select **Export**. You will then be prompted as to where you would like to restore the contents of the folder to.

How to restore files that have been encrypted on DropBox folders

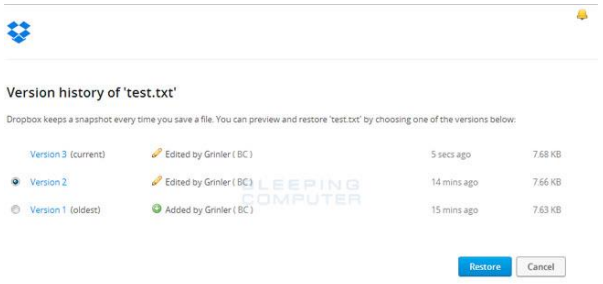
If you have DropBox mapped to a drive letter on an infected computer, CryptoLocker will attempt to encrypt the files on the drive. DropBox offers free versioning on all of its accounts that will allow you to restore encrypted files through their website. Unfortunately, the restoral process offered by DropBox only allows you to restore one file at a time rather than a whole folder. If you need instructions on restoring an entire folder in DropBox, please click **here**.

To restore a file, simply login to the DropBox web site and navigate to the folder that contains the encrypted files you wish to restore. Once you are in the folder, right-click

on the encrypted file and select Previous Versions as shown in the image below.



When you click on Previous versions you will be presented with a screen that shows all versions of the encrypted file.



Select the version of the file you wish to restore and click on the **Restore** button to restore that file.

Unfortunately the process outlined above can be very time consuming if there are many folder to restore. In order to restore an entire folder of encrypted files, you can use the dropbox-restore python script located **here**. Please note that this script requires Python to be installed on the encrypted computer to execute the script. Instructions on how to use this script can be found in the **README.md** file for this project.

How to find files that have been encrypted by CryptoLocker

There are currently three method that you can use to generate a list of files that have been possible encrypted. Each of these methods is outlined below.

Method 1: ListCriLock

If you wish to generate a list of files that have been encrypted, you can download this tool that I have created:

http://download.bleepingcomputer.com/grinler/ListCrilock.exe

When you run this tool it will generate a log file that contains a list of all encrypted files found under the HKCU\Software\CryptoLocker\Files or the HKCU\Software\CryptoLocker_0388\Files key. Once it has completed it will automatically open this log in Notepad.

Method 2: Windows PowerShell

Another method is to use the Windows PowerShell (thanks **prsgroup**):

For systems with PowerShell, you can dump the list of files in the CryptoLocker registry key using the following command:

```
(Get-Item HKCU:\Software\CryptoLocker\Files).GetValueNames().Replace("?","\") | Out-File CryptoLockerFiles.txt -Encoding unicode
```

Make sure to include the "-Encoding unicode" parameter to ensure that filenames with Unicode characters are preserved.

Method 3: Omnispear's CryptoLocker Scan Tool

You can use the **CryptoLocker Scan Tool** from Omnispear to search for and list encrypted files found on your computer. This program will look for certain file identifiers that are normally found in a file based on that file's extension. If the file identifier does not exist it would indicate that the file is either encrypted or corrupted.

How to determine which computer is infected with CryptoLocker on a network

On a large network, determining the computer that is infected with CryptoLocker can be difficult. Some infected users have reporter that encrypted files will have their ownership changed to the user that the CryptoLocker program is running under. You can then use this login name to determine the infected computer.

You can also examine your network switches and look for the ports that have lights that are continuously blinking or show very heavy traffic. You can then use this to further narrow down what computers may be infected.

How to prevent your computer from becoming infected by CryptoLocker

You can use the Windows Group or Local Policy Editor to create Software Restriction Policies that block executables from running when they are located in specific paths. For more information on how to configure Software Restriction Policies, please see these articles from MS:

http://support.microsoft.com/kb/310791
http://technet.microsoft.com/en-us/library/cc786941(v=ws.10).aspx

The file paths that have been used by this infection and its droppers are:

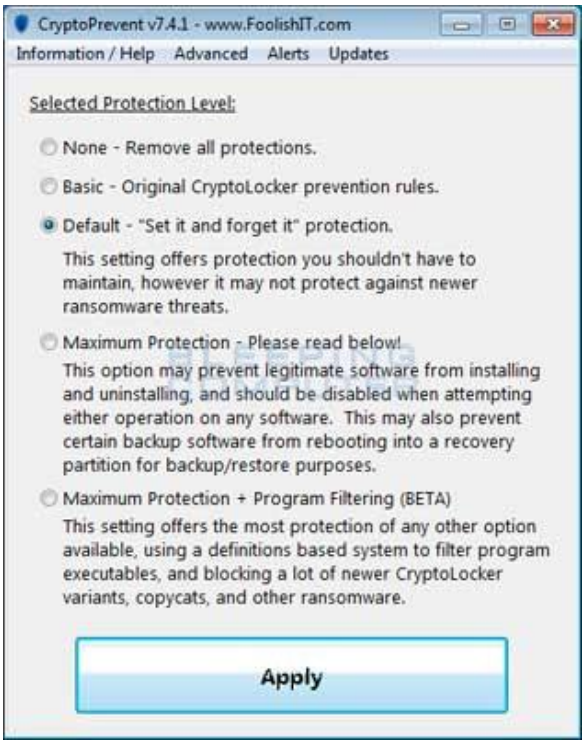
C:\Users\<User>\AppData\Local\<random>.exe (Vista/7/8)
C:\Users\<User>\AppData\Local\<random>.exe (Vista/7/8)
C:\Documents and Settings\<User>\Application Data\<random>.exe (XP)
C:\Documents and Settings\<User>\Local Application Data\<random>.exe (XP)

In order to block the CryptoLocker you want to create Path Rules so that they are not allowed to execute. To create these Software Restriction Policies, you can either use the **CryptoPrevent** tool or add the policies **manually** using the Local Security Policy Editor or the Group Policy Editor. Both methods are described below.

Note: If you are using Windows Home or Windows Home Premium, the Local Security Policy Editor will not be available to you. Instead we suggest you use the **CryptoPrevent** tool, which will automatically set these policies for you.

How to use the CryptoPrevent Tool:

FoolishIT LLC was kind enough to create a free utility called CryptoPrevent that automatically adds the suggested Software Restriction Policy Path Rules listed above to your computer. This makes it very easy for anyone using Windows XP SP 2 and above to quickly add the Software Restriction Policies to your computer in order to prevent CryptoLocker and Zbot from being executed in the first place. This tool is also able to set these policies in all versions of Windows, including the Home versions.



A new feature of CryptoPrevent is the option to whitelist any existing programs in %AppData% or %LocalAppData%. This is a useful feature as it will make sure the restrictions that are put in place do not affect legitimate applications that are already installed on your computer. To use this feature make sure you check the option labeled **Whitelist EXEs already located in**

%appdata% / %localappdata% before you press the **Block** button.

You can download CryptoPrevent from the following page:

http://www.foolishit.com/download/cryptoprevent/

For more information on how to use the tool, please see this page:

http://www.foolishit.com/vb6-projects/cryptoprevent/

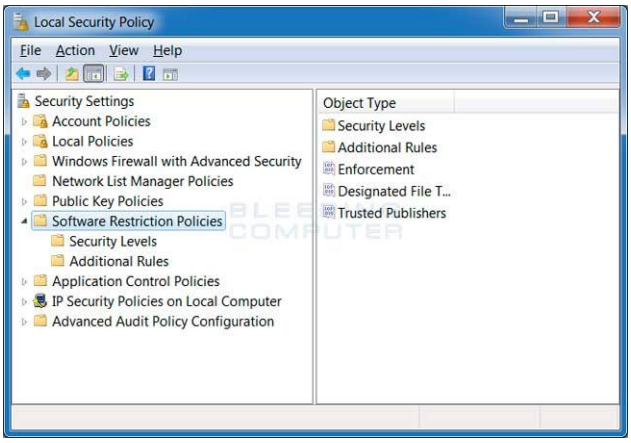
Tip: You can use CryptoPrevent for free, but if you wish to **purchase** the premium version you can use the coupon code **bleeping30off** to get 30% off. The premium version includes automatic and silent updating of application and definitions on a regular schedule, email alerts when an application blocked, and custom allow and block policies to fine-tune your protection.

Once you run the program, simply click on the **Apply Protection** button to add the default Software Restriction Policies to your computer. If you wish to customize the settings, then please review the checkboxes and change them as necessary. If CryptoPrevent causes issues running legitimate applications, then please see **this section** on how to enable specific applications. You can also remove the Software Restriction Policies that were added by clicking on the **Undo** button.

How to manually create Software Restriction Policies to block CryptoLocker:

In order to manually create the Software Restriction Policies you need to be using Windows Professional or Windows Server. If you want to set these policies for a particular computer you can use the Local Security Policy Editor. If you wish to set these policies for the entire domain, then you need to use the Group Policy Editor. Unfortunately, if you are a Windows Home user, the Local Policy Editor ir not available and you should use the**CryptoPrevent** tool instead to set these policies. To open the Local Security Policy editor, click on the **Start** button and type **Local Security Policy** and select the search result that appears. You can open the Group Policy Editor by typing **Group Policy** instead. In this guide we will use the Local Security Policy Editor in our examples.

Once you open the Local Security Policy Editor, you will see a screen similar to the one below.



Once the above screen is open, expand **Security Settings** and then click on the **Software Restriction Policies** section. If you do not see the items in the right pane as shown above, you will need to add a new policy. To do this click on the **Action** button and select **New Software Restriction Policies**. This will then enable the policy and the right pane will appear as in the image above. You should then click on the **Additional Rules** category and then right-click in the right pane and select **New Path Rule...**. You should then add a Path Rule for each of the items listed below.

If the Software Restriction Policies cause issues when trying to run legitimate applications, you should see **this section** on how to enable specific applications.

Below are a few Path Rules that are suggested you use to not only block the infections from running, but also to block attachments from being executed when opened in an e-mail client.

Block CryptoLocker executable in %AppData%

Path: %AppData%*.exe
Security Level: Disallowed
Description: Don't allow executables to run from %AppData%.

Block CryptoLocker executable in %LocalAppData%

Path if using Windows XP: %UserProfile%\Local Settings*.exe

Path if using Windows Vista/7/8: %LocalAppData%*.exe
Security Level: Disallowed
Description: Don't allow executables to run from %AppData%.

Block Zbot executable in %AppData%

Path: %AppData%.exe**
Security Level: Disallowed
Description: Don't allow executables to run from immediate subfolders of %AppData%.

Block Zbot executable in %LocalAppData%

Path if using Windows XP: %UserProfile%\Local Settings.exe**
Path if using Windows Vista/7/8: %LocalAppData%.exe**
Security Level: Disallowed
Description: Don't allow executables to run from immediate subfolders of %AppData%.

Block executables run from archive attachments opened with WinRAR:

Path if using Windows XP: %UserProfile%\Local Settings\Temp\Rar.exe**
Path if using Windows Vista/7/8: %LocalAppData%\Temp\Rar.exe**
Security Level: Disallowed
Description: Block executables run from archive attachments opened with WinRAR.

Block executables run from archive attachments opened with 7zip:

Path if using Windows XP: %UserProfile%\Local Settings\Temp\7z.exe**
Path if using Windows Vista/7/8: %LocalAppData%\Temp\7z.exe**
Security Level: Disallowed
Description: Block executables run from archive attachments opened with 7zip.

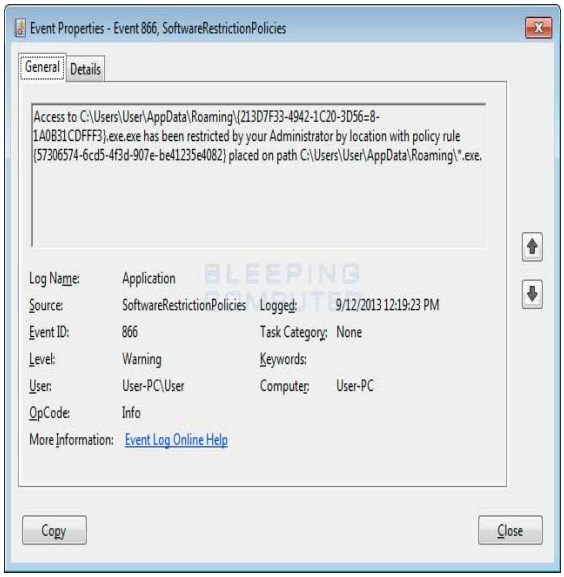
Block executables run from archive attachments opened with WinZip:

Path if using Windows XP: %UserProfile%\Local Settings\Temp\wz.exe**
Path if using Windows Vista/7/8: %LocalAppData%\Temp\wz.exe**
Security Level: Disallowed
Description: Block executables run from archive attachments opened with WinZip.

Block executables run from archive attachments opened using Windows built-in Zip support:

Path if using Windows XP: %UserProfile%\Local Settings\Temp*.zip*.exe
Path if using Windows Vista/7/8: %LocalAppData%\Temp*.zip*.exe
Security Level: Disallowed
Description: Block executables run from archive attachments opened using Windows built-in Zip support.

You can see an event log entry and alert showing an executable being blocked:

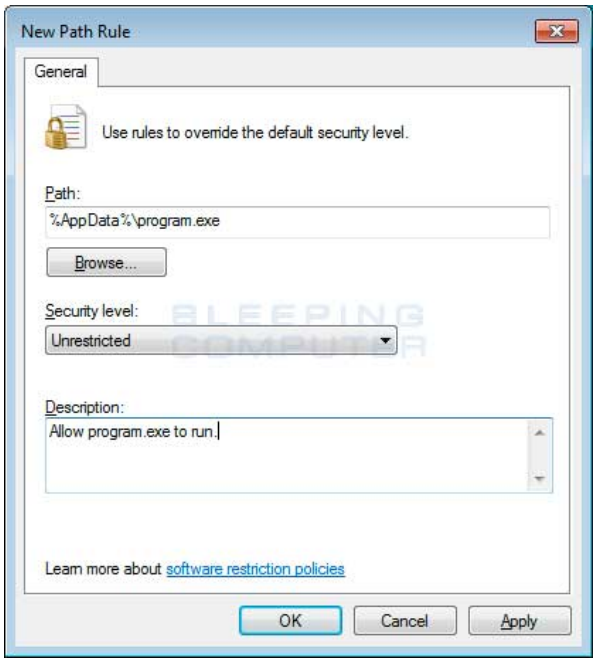


If you need help configuring this, feel free to ask in the **CryptoLocker help topic**.

How to allow specific applications to run when using Software Restriction Policies

If you use Software Restriction Policies, or CryptoPrevent, to block CryptoLocker you may find that some legitimate applications no longer run. This is because some companies mistakenly install their applications under a user's profile rather than in the Program Files folder where they belong. Due to this, the Software Restriction Policies will prevent those applications from running.

Thankfully, when Microsoft designed Software Restriction Policies they made it so a Path Rule that specifies a program is allowed to run overrides any path rules that may block it. Therefore, if a Software Restriction Policy is blocking a legitimate program, you will need to use the **manual steps** given above to add a Path Rule that allows the program to run. To do this you will need to create a Path Rule for a particular program's executable and set the Security Level to **Unrestricted** instead of Disallowed as shown in the image below.



Once you add these Unrestricted Path Rules, the specified applications will be allowed to run again.

CryptoLocker 2.0: New version or Copycat?

ESET wrote a **blog post** about a new infection called CryptoLocker 2.0. Though this infection appears to be a new version of the CryptoLocker there are key differences that hint that this is just a copycat trying to benefit from the fame of the original infection.

The main differences between the two are:

- A major indication that this is a copycat is that it is programmed using a completely different language. The original is programmed in native C++ code that did not have any prerequisites to execute on a computer. CryptoLocker 2.0 is written in C# that requires the .NET Framework 4.0 to run.
- This malware contains a cryptocoin miner called BFGMiner that could allow it to mine Bitcoins, and other crypto coins, using the CPU power or graphic card on your computer. The mined coins would then go into the wallet of the malware developer.
- Based on strings found in the executable, this malware appears to be able perform DDOS attacks.
- The malware does not use a domain generation algorithm, but instead hard codes the C2 server's address.

- Uses a different encryption type then the original CryptoLocker

When installed, the dropper will install the main executable as:

```
%AppData%\Microsoft\msunet.exe
```

It will then create the following registry keys to autostart the program in normal mode and safe mode.

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\MSUpdate
%AppData%\Microsoft\msunet.exe
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce\*MSUpdate
%AppData%\Microsoft\msunet.exe
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
C:\Windows\system32\userinit.exe,,%AppData%\Microsoft\msunet.exe
```

The infection encrypts files with the following extensions;

```
3fr, accdb, txt, ai, arw, bay, cdr, cer, cr2, eps, erf, indd, mp3, mp4, jpe, jpg, kdc, mdb, mdf, mef, mrw, nef, crt, crw, dbf, dcr, der, dng, doc, docm, docx, dwg, dxf, dxg, rwl, srf, srw, wb2, wpd, wps, xlk, nrw, odb, odm, odp, ods, odt, orf, p12, p7b, p7c, pdd, xls, xlsb, xlsm, xlsx, pef, pem, pfx, ppt, pptm, pptx, psd, pst, ptx, r3d, raf, raw, rtf
```

Over all, the developer of this malware drastically changed the approach of the original CryptoLocker. Instead of focusing on encrypting files and getting paid for the decryption key, this infection tries to throw the kitchen sink at you in order to maximize revenue.

CryptoLocker Timeline

September 6th, 2013	The first reported appearance of CryptoLocker was reported by a member of our forum in the**Cryptolocker Hijack program** topic. The user was reporting a popup window called CryptoLocker and how all of their data files were encrypted. New reports immediately started flooding in as other infected users were able to find the topic.
September 9th, 2013	Fabian Wosar of **Emsisoft** was the first to reverse-engineer the CryptoLocker infection. His analysis was posted on the **kernelmode.info** forum. A more formal write up was later posted on Emsisoft's blog in the blog post **CryptoLocker – a new ransomware variant**.
September 10th, 2013	The ListCrilock tool was released by **BleepingComputer.com** that can be used to export a list of encrypted files from the Registry.
September 12th, 2013	Suggestion to use Software Restriction Policies to block CryptoLocker executables was **posted**.
October 8th, 2013	Connection between Zbot being the downloaded for CryptoLocker was **reported**.
October 10th, 2013	BleepingComputer.com became the subject of a large DNS amplification **DDOS attack**. This was presumably due to the information we were disclosing about the connection between Zbot and CryptoLocker.
October 14th, 2013	BleepingComputer.com created this CryptoLocker Ransomware Information Guide and FAQ to be a compilation of all known information about this infection.
October 18th, 2013	CryptoLocker becomes mainstream news as various AV vendors and news companies start reporting about the infection.
October 18th, 2013	First **report** of CryptoLocker Command & Control servers started to display a message from the developers on their home page. Screenshot of this home page can be found **here**.
October 18th, 2013	Nicholas Shaw, CEO and developer of **Foolish IT**, released **CryptoPrevent** that provides an easy to use program to create the necessary Software Restriction Policies on a computer.
October 25th, 2013	Omnispear released the **CryptoLocker Scan Tool** that scans your hard drives

	for files that do not have the proper file identifiers in them. If a file is discovered that does not have the proper file identified based on its extension, the tool will report it as possible encrypted.
October 29th, 2013	CryptoLocker Command & Control server home page changed the message from the developer. Screenshot of the new message can be found **here**.
November 1st, 2013	**CryptoLocker Decryption Service** was released by the malware developers. This new decryption service allowed an infected user to upload an encrypted file and purchase a decryption key and decrypter for 10 bitcoins.
November 4th, 2013	**CryptoLocker Decryption Service** was updated to state that a user can still pay 2 bitcoins to purchase their decryption service as long as they are within the initial 72 hour period. If they fail to pay the ransom within 72 hours they will then have to pay 10 bitcoins to purchase the decryption key and decrypter.
November 5th, 2013	**SurfRight** released a new tool called **CryptoGuard** that monitors the file system for suspicious file operations (CryptoGuard is a driver, installed by HitmanPro.Alert). When suspicious behavior is detected, the malicious code is blocked (write, delete, rename is revoked) and an Alert is presented to the user. So even while ransomware is active, it can't harm your files.
June 2nd, 2014	Information about **Operation Tovar** was released that took down the Gameover distribution network that distributed CryptoLocker.
August 6th, 2014	**Decryption keys** discovered during Operation Tovar were made available by FireEye and Fox IT.

Threat Classification:

- **Information on Ransomware Programs**

Advanced information:

View CryptoLocker files.
View CryptoLocker Registry Information.

Symptoms that may be in a HijackThis Log:

O4 - HKCU\..\Run: [<random>] C:\Users\<user>\AppData\Roaming\<random>\<random>.exe
O4 - HKCU\..\Run: [CryptoLocker] C:\Users\<User>\AppData\Roaming\<Random>.exe
O4 - HKCU\..\RunOnce: [*CryptoLocker] C:\Users\<User>\AppData\Roaming\<Random>.exe

Guide Updates:

10/15/13 - Initial guide creation
10/16/13 - Fleshed out the native previous versions feature.
10/19/13 - Minor updates
10/20/13 - Updated with more info including the new tool CryptoPrevent
10/22/13 - Updated guide with updates on CryptoPrevent, new install paths, new Registry key locations, and the message on the Command & Control Server.
10/23/13 - Fixed %Temp% path rules and added info about known Bitcoin payment addresses.
10/29/13 - Updated C2 message.
11/02/13 - Added info about new CryptoLocker decryption server and how the infection tries to delete shadow copies.
11/05/13 - Added more information about the decryption tool you receive when you pay the ransom.
11/08/13 - Big update. Added information about restoring from dropbox, exe hijack to remove shadow copies, a timeline of this infection and related tools, and added more prevention tools.
11/21/13 - Added more information about paths and registry keys that are being used. Also added known list of spam subjects.
12/20/13 - Updated for the CryptoLocker 2.0 copycat.

08-06-14 - Updated with information on the FireEye/Fox IT key retrieval and decrypter
09/19/14 - Added info to the top of the page about TorrentLocker.
10/31/14 - Updated info about CryptoPrevent

This is a self-help guide. Use at your own risk.

BleepingComputer.com can not be held responsible for problems that may occur by using this information. If you would like help with any of these fixes, you can ask for malware removal assistance in our Virus, Trojan, Spyware, and Malware Removal Logs forum.

If you have any questions about this self-help guide then please post those questions in our Am I infected? What do I do? and someone will help you.

Associated CryptoLocker Files:

%AppData%\<random>.exe
%AppData%\<random>\<random>.exe (zbot)
%LocalAppData%\<random>.exe

File Location Notes:

%AppData% refers to the current users Application Data folder. By default, this is C:\Documents and Settings\<Current User>\Application Data for Windows 2000/XP. For Windows Vista and Windows 7 it is C:\Users\<Current User>\AppData\Roaming.

%LocalAppData% refers to the current users Local settings Application Data folder. By default, this is C:\Documents and Settings\<Current User>\Local Settings\Application Data for Windows 2000/XP. For Windows Vista, Windows 7, and Windows 8 it is C:\Users\<Current User>\AppData\Local.

Associated CryptoLocker Windows Registry Information:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "CryptoLocker"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "CryptoLocker_<version>"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce "*CryptoLocker"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "<Random>"