The latest blog on this nasty thing is at http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information

Some hope on recovering the encrypted file is at http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information#shadow

Details on how to use CryptoPrevent can be found at http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information#cryptoprevent

Your want the internal called **How to prevent your computer from becoming infected by CryptoLocker** which is # 17 in the table of contents

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

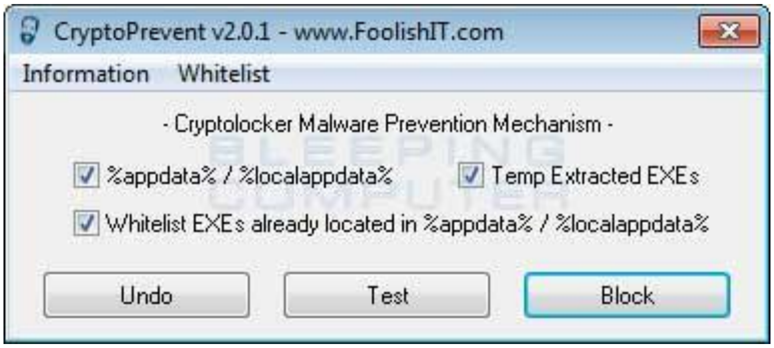
The file paths that have been used by this infection and its droppers are:

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 and Zbot infections 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**. Both methods are described below.

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 below 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.



- Cryptolocker Malware Prevention Mechanism -

☑ %appdata% / %localappdata%
☑ Temp Extracted EXEs
☑ Whitelist EXEs already located in %appdata% / %localappdata%

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/

Once you run the program, simply click on the **Block** button to add the Software Restriction Policies to your computer. 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.