DocWatch 2.0

A Windows monitoring application that alerts when excessive file activity occurs and detects Crypto type malware attacks

[Administrators Guide]

Michael A. Todd (mAt)

Revision 9/19/2015

This Guide is intended for either personal usage by individuals or for administrator usage in corporate environments. It details the theory and operation of the Doc Watch program. ©2015

Contents

DocWatch – A Windows Document File Watcher

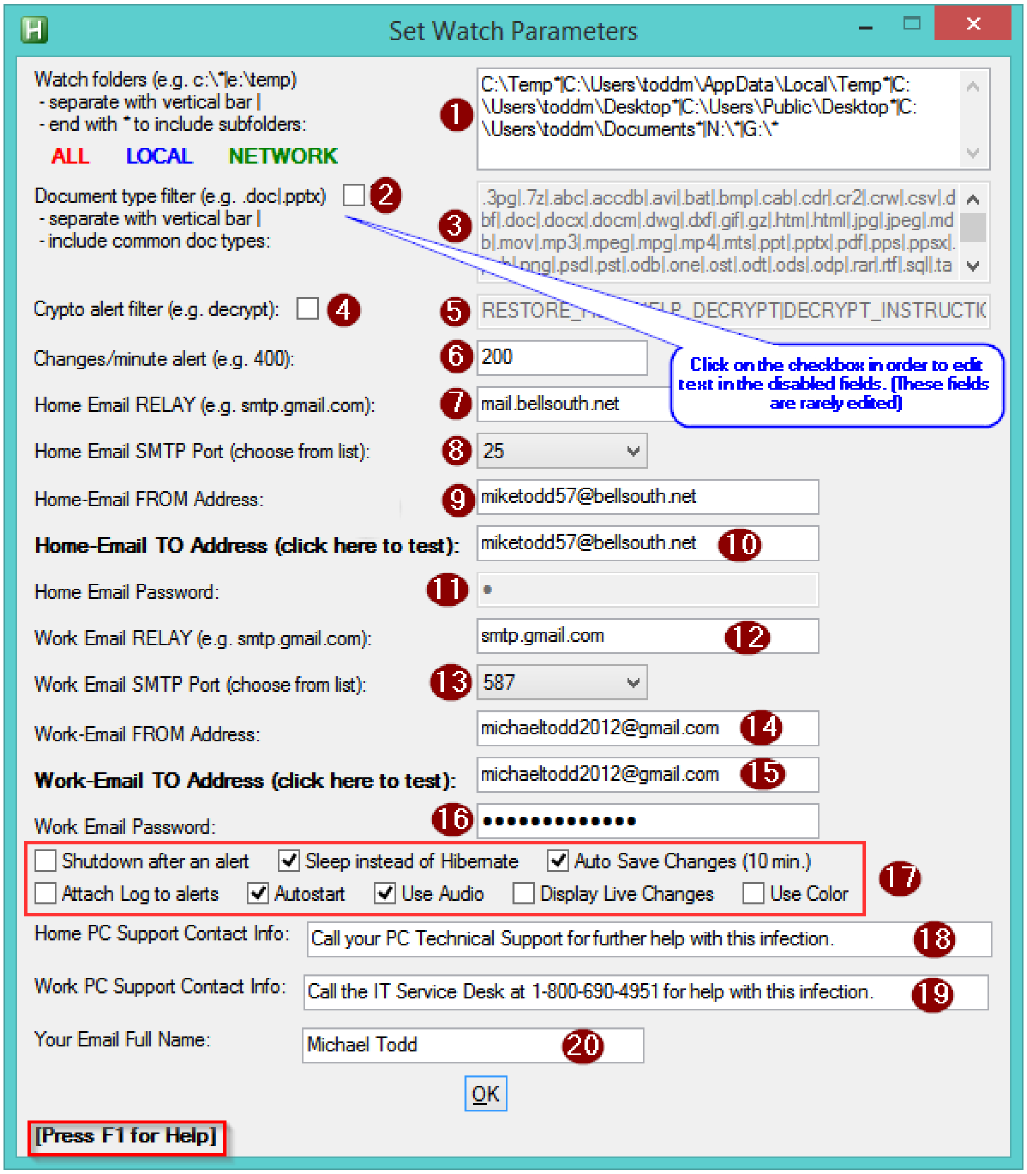
DocWatch warns when malware is affecting user documents and sends email alerts to the document owner or to an IT administrator. It looks for specific filenames and for excessive document activity.

Installation:

Extract the contents of the DocWatch.zip file to a folder of your choice. In this guide the Desktop folder will be used to run the program from. The only files in the zip are DocWatch.exe and this Users Guide. This guide is embedded inside the program and will be displayed whenever F1 is pressed from the main window.

Launching / Initial Setup:

Doc Watch.exe After double-clicking on the program, you will see the initial Setup window. The initial setup parameters will supplied by the program. *Each item is covered by number in detail starting on the next page.*



Set Watch Parameters

Watch folders (e.g. c:\*|e:\temp)
- separate with vertical bar |
- end with * to include subfolders:

ALL LOCAL NETWORK

1 C:\Temp*|C:\Users\toddm\AppData\Local\Temp*|C:\Users\toddm\Desktop*|C:\Users\Public\Desktop*|C:\Users\toddm\Documents*|N:\*|G:\*

Document type filter (e.g. .doc|.pptx) □ 2
- separate with vertical bar |
- include common doc types:

3 .3pg|.7z|.abc|.accdb|.avi|.bat|.bmp|.cab|.cdr|.cr2|.crw|.csv|.dbf|.doc|.docx|.docm|.dwg|.dxf|.gif|.gz|.htm|.html|.jpg|.jpeg|.mdb|.mov|.mp3|.mpeg|.mpg|.mp4|.mts|.ppt|.pptx|.pdf|.pps|.ppsx|.b|.png|.psd|.pst|.odb|.one|.ost|.odt|.ods|.odp|.rar|.rtf|.sql|.ta

Crypto alert filter (e.g. decrypt): □ 4

5 RESTORE_F ELP_DECRYPT|DECRYPT_INSTRUCTI(

Click on the checkbox in order to edit text in the disabled fields. (These fields are rarely edited)

Changes/minute alert (e.g. 400): 6 200

Home Email RELAY (e.g. smtp.gmail.com): 7 mail.bellsouth.net

Home Email SMTP Port (choose from list): 8 25

Home-Email FROM Address: 9 miketodd57@bellsouth.net

Home-Email TO Address (click here to test): miketodd57@bellsouth.net 10

Home Email Password: 11 •

Work Email RELAY (e.g. smtp.gmail.com): smtp.gmail.com 12

Work Email SMTP Port (choose from list): 13 587

Work-Email FROM Address: michaeltodd2012@gmail.com 14

Work-Email TO Address (click here to test): michaeltodd2012@gmail.com 15

Work Email Password: 16 ••••••••••••••

17
□ Shutdown after an alert ☑ Sleep instead of Hibernate ☑ Auto Save Changes (10 min.)
□ Attach Log to alerts ☑ Autostart ☑ Use Audio □ Display Live Changes □ Use Color

Home PC Support Contact Info: Call your PC Technical Support for further help with this infection. 18

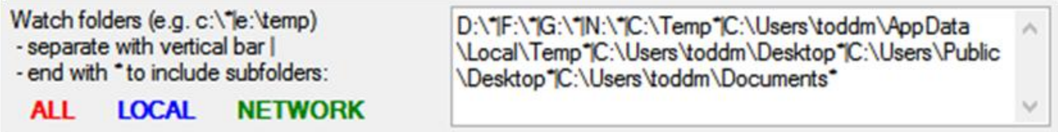
Work PC Support Contact Info: Call the IT Service Desk at 1-800-690-4951 for help with this infection. 19

Your Email Full Name: Michael Todd 20

[Press F1 for Help]

The initial Watch Folders are based on the hard disk, removable and network drives for which your computer has access. The default Document Filter contains the most common types of documents. Likewise, the Crypto Filter contains the most recent filenames used by several crypto related type of malware. If you only use the program at home then made sure the Home Email Relay, From Suffix and To are filled in correctly. If you will use the program at work then fill in the Work Email items. Home/Office users will need to fill in both sets of items.

1. Watch Folders – this is the list of drives with optional folder names that you want the program to watch for file changes. If you want to just watch your C drive Temp folder, then enter C:\Temp. If you also want to watch any folders under Temp then add an asterisk at the end, like C:\Temp*. Separate all entries with vertical bars (|) except at the very end. If you want to watch your whole hard disk C then enter C:\*. This value defaults to all drives your system is connected to and always adds common document folders for the logged in user (i.e. C:\Users\SmithJ\Desktop). The single letters are separate disk drives and added the first time the program is run, they represent any external or network drives that your computer has access to. The C:\Users entries are added automatically based on the current user and cover the common folders where users have documents.
   Quick Watch Settings – You can easily switch between All Drives, Local Drives (fixed plus removable) and Network only Drives by clicking on the ALL, LOCAL or NETWORK labels.

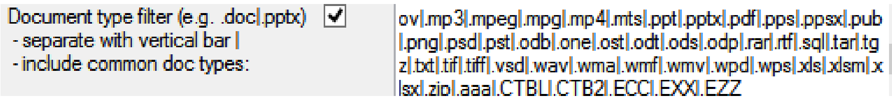


Watch folders (e.g. c:\*|e:\temp)
- separate with vertical bar |
- end with * to include subfolders:

ALL LOCAL NETWORK

D:\*|F:\*|G:\*|N:\*|C:\Temp*|C:\Users\toddm\AppData
\Local\Temp*|C:\Users\toddm\Desktop*|C:\Users\Public
\Desktop*|C:\Users\toddm\Documents*

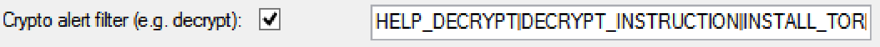
2. Document Type Filters Enable checkbox – if you need to add or edit the Type Filters then click on the checkbox to turn it on. Turning it back off makes the edit field read only again. [This value is not saved to disk. It will always be read only when you open the Setup window.]



Document type filter (e.g. .doc|.pptx) ☑
- separate with vertical bar |
- include common doc types:

ov|.mp3|.mpeg|.mpg|.mp4|.mts|.ppt|.pptx|.pdf|.pps|.ppsx|.pub
|.png|.psd|.pst|.odb|.one|.ost|.odt|.ods|.odp|.rar|.rtf|.sql|.tar|.tg
z|.txt|.tif|.tiff|.vsd|.wav|.wma|.wmf|.wmv|.wpd|.wps|.xls|.xlsm|.x
lsx|.zip|.aaa|.CTBL|.CTB2|.ECC|.EXX|.EZZ

3. Document Type Filters – these are all of the types of files the program pays attention to. If you are creating a New Word document, Renaming or Deleting one, then it will be logged if you have .doc and .docx in the list of Type Filters. These are all separated by vertical bars (|). The default values cover most all common document file types. These are read only by default since they are rarely changed.
4. Crypto Alert Filter Enable checkbox – Since these values are very specific, editing them is disabled unless you click on the checkbox.
5. Crypto Alert Filter – this value contains filenames that associated with Crypto malware. They are a used to check against each new or renamed document. If a filename matches one of these values then you will be prompted that you probably have Crypto malware activity on your computer. An email will then be sent to the address specified in item 10 or item 13. Since these values are very specific, editing them is disabled.



Crypto alert filter (e.g. decrypt): ☑ HELP_DECRYPT|DECRYPT_INSTRUCTION|INSTALL_TOR|

6. Changes / minute Alert – since new variations of malware come out regularly it is not possible to keep the Crypto filter continuously updated. Since all Crypto related malware encrypts all of the document files on your local system (and network drives mapped to a letter), it is a very intensive file activity. By monitoring how many New and Renamed files there are per minute, this program can alert you to possible malware activity. This value is somewhat subjective. If you don't work with a lot of files regularly, mainly through copying, pasting, moving or backing them up, then you can leave this at 100 changes per minute. DocWatch will not display any prompts until there have been 3 minutes with at least 100 changes each minute. So, the default setting will generate an email once 300 or more changes have been made in a 3 minute period. If you were to set it to 300 then the

email alert would happen after 900 changes in 3 minutes. The rule of thumb is to set a higher value if you are seeing alerts during normal usage of the computer.

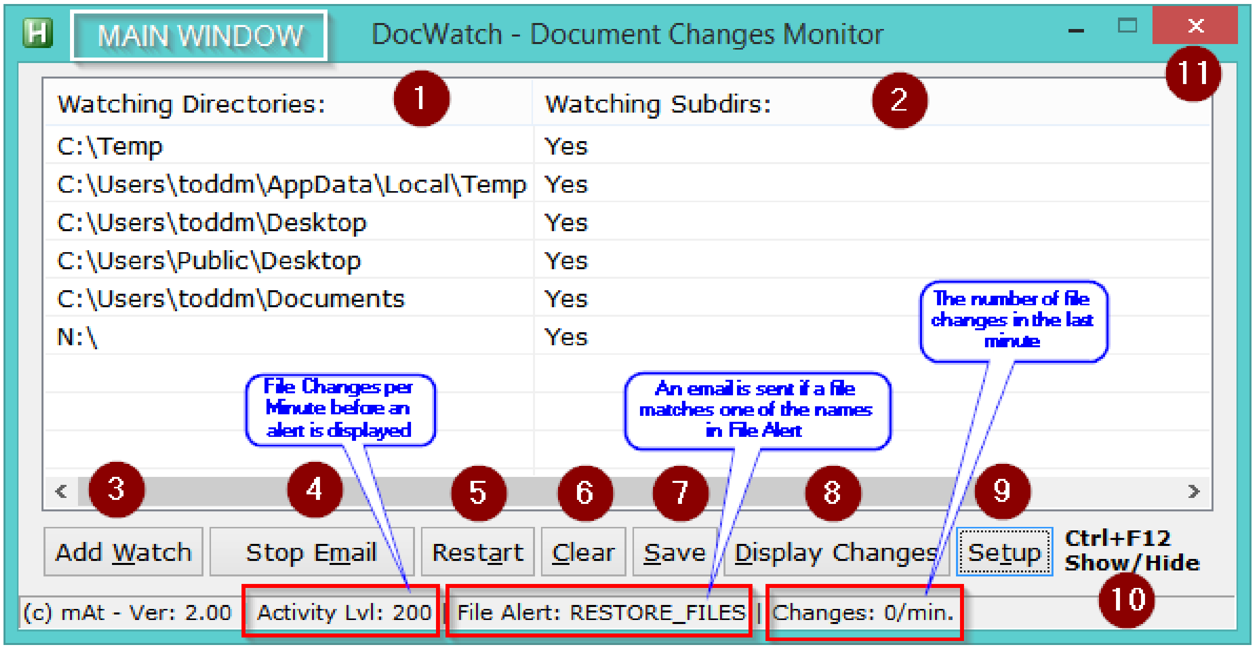
7. Home Email Relay – Users may want to look at this webpage as it contains most of the common email providers along with their Relay server addresses.
8. Home Email SMTP Port – You can configure your email to use port 25, 465 (SSL) or 587 (TLS). The last two port settings enable encryption of emails and require a password.
9. Home Email From – Enter the FROM address for your email. Usually the same as TO.
10. Home Email To – Enter the send TO email address. [note: you may click on the Home-Email label to test]
11. Home Email Password – When the SMTP port is set to 25, the password is disabled. When using ports 465 or 587, enter the email password here. [Note – email passwords are never displayed, they are encrypted before saving them to the DocWatch.ini file. They are only in plain text within the DocWatch process while it is running. So no one is going to get to the password.]
12. Work Email Relay – Users may want to look at this webpage as it contains most of the common email providers along with their Relay server addresses.
13. Work Email SMTP Port – You can configure your email to use port 25, 465 (SSL) or 587 (TLS). The last two port settings enable encryption of emails and require a password.
14. Work Email From – Enter the send TO email address. [note: you may click on the Home-Email label to test]
15. Work Email To – Enter the send TO email address. [note: you may click on the Home-Email label to test]
16. Work Email Password – When the SMTP port is set to 25, the password is disabled. When using ports 465 or 587, enter the email password here. [See Note above]
17. Various Program Feature Toggles:
    a. Shutdown after an alert [PCs only, not Servers] – depending on where the computer resides users can decide whether or not to put the computer in Standby or Hibernate in order to stop malware file encryption of both local and network documents. It is recommended to leave this enabled after becoming familiar with the program. After sending an email, the PCs network connection is also temporarily disabled except if you are running the program from a Windows Server. You will hear audio messages regarding the Crypto malware that was detected and that the computer will be put in Sleep.
    b. Sleep instead of Hibernate [PCs only, not Servers] – While testing the program, it is advisable to check this so the computer will go into Sleep/Standby mode after a Crypto alert. It is much faster to come out of Sleep than Hibernate which turns off the computer.
    c. Auto Save Change List (10 min.) – So that the internal Change List doesn’t grow very large, this option will log the changes then clear the list every 10 minutes.
    d. Attach Log Files to Email Alerts – By default, up to 10 minutes of changes added to the List View will be inserted into the body of email alerts. Since this can be several hundred files, this option can be turned off, but is not recommended.
    e. AutoStart – When you click on AutoStart then click OK to save settings, the program will add a shortcut to your Startup folder. This is highly recommended so that DocWatch runs whenever you start your computer.
    f. UseAudio – In addition to the initial audio announcing the Setup window, there are other times when audio can be used. Whenever the computer file activity reaches the Activity Level for 3 minutes in a row, there is an audio warning. Whenever a Crypto malware file is created, another audio prompt announces that and also lets you know the computer needs to be shutdown until PC Support can look at it.
    g. Display Live Changes – Until you are familiar with the operation of the program you may opt to display the active List View of document changes. (See this expanded Main window on page xx.)

h. Use Color – Initially, when using the List View displays every item in black and white. But, if this is checked then Deleted/Renamed From files show up in Silver, Crypto-related files show up in Red and High activity documents show up in Cyan and in Lime colors. Takes more CPU power to keep the list colorized, the default is off.

18. Home PC Support Contact Info – Enter the name/description/phone number of who you would contact for Home computer issues.
19. Work PC Support Contact Info – Enter the name/description/phone number of who you contact for computer support at your workplace.
20. Your Email Full Name – When using secure email sends you will need to enter your Full Name.
21. Press F1 for Help – Any time the Main or the Setup windows are displayed, you may press F1 to display a copy of this guide.
22. OK – Click on the OK button to save your changes or click on the upper right X to just close the Setup window.

Main Window:

Click OK to save these parameters and the main window will be displayed.



Watching Directories:	Watching Subdirs:
C:\Temp	Yes
C:\Users\toddm\AppData\Local\Temp	Yes
C:\Users\toddm\Desktop	Yes
C:\Users\Public\Desktop	Yes
C:\Users\toddm\Documents	Yes
N:\	Yes

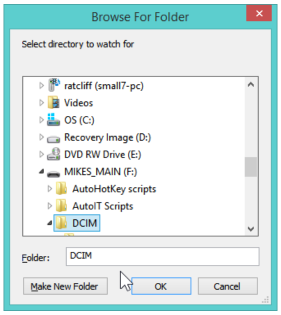
(c) mAt - Ver: 2.00 | Activity Lvl: 200 | File Alert: RESTORE_FILES | Changes: 0/min.

MAIN WINDOW
DocWatch - Document Changes Monitor
1
2
11
The number of file changes in the last minute
File Changes per Minute before an alert is displayed
An email is sent if a file matches one of the names in File Alert
3
4
5
6
7
8
9
Add Watch
Stop Email
Restart
Clear
Save
Display Changes
Setup
Ctrl+F12 Show/Hide
10

The areas of this window are described below. Under normal usage, this window is hidden from view.

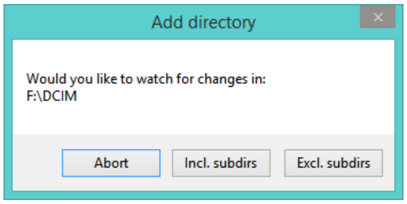
1. List of Watched Folders – In the top half of the window, the currently watched folders are displayed. Double-clicking on any of them will open Windows Explorer to that drive/folder. (See page xx for a picture of this List View) In the bottom half of the window changes to select documents will be displayed. Only file types matching the Document Type Filters will be listed. And only when they are New, Renamed From/To or Deleted. When a filename matches one of the Crypto Alert filters then messages will be displayed and an email sent. The status bar color will also changed to Red as shown on the next page.
2. Watched Subdirectories – This column shows Yes for directories whose subdirectories are also being watched. In order to watch a whole hard drive or mapped network drives just enter something like C:\* or H:\*.

3. Add Watch Directory – clicking on Add Watch displays a Folder browser window. Choose a folder to add and click OK. You may Abort the operation or choose to Include / Exclude subdirectories by clicking a button. The program will Restart then display the newly added folder.

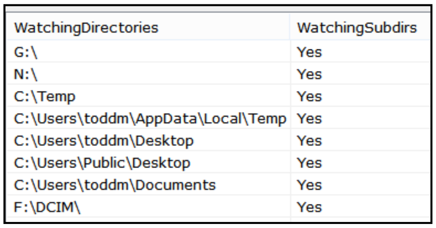

Browse For Folder

Select directory to watch for

Folder: DCIM


Add directory

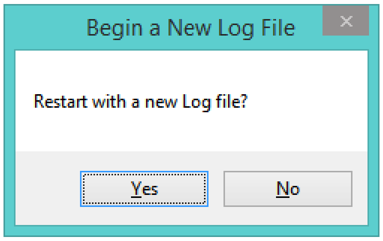
Would you like to watch for changes in:
F:\DCIM



WatchingDirectories	WatchingSubdirs
G:\	Yes
N:\	Yes
C:\Temp	Yes
C:\Users\toddm\AppData\Local\Temp	Yes
C:\Users\toddm\Desktop	Yes
C:\Users\Public\Desktop	Yes
C:\Users\toddm\Documents	Yes
F:\DCIM\	Yes

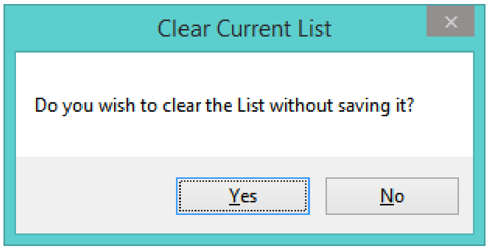
4. Stop Email – if you are going to work with a lot of files through backup/restore or just moving folders around, you should click Stop Email so that the program doesn't display unnecessary warnings or send email alerts until you are finished. When you click on Stop Email, the button changes to display Restart Email.

5. Restart – After an Activity or Crypto Alert happens you can use Restart to reinitialize the program and reset the color of the StatusBar. You will be asked if you want to begin with a new Log file. An Archive Log file is created if Yes is clicked.

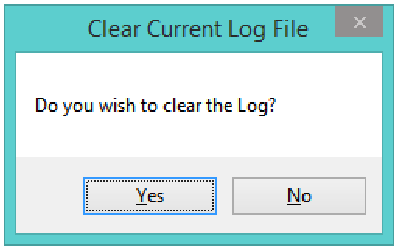

Begin a New Log File

Restart with a new Log file?

6. Clear List – the Changes List can be cleared manually or a 10 minute timer can be set to do it. An Archive Log file is created if Yes is clicked.

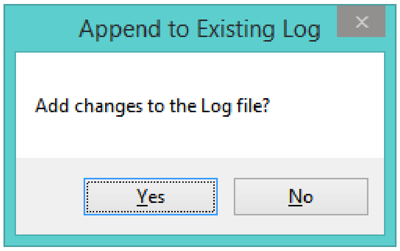

Clear Current List

Do you wish to clear the List without saving it?


Clear Current Log File

Do you wish to clear the Log?

7. Save – Saves the current list to a Log file.

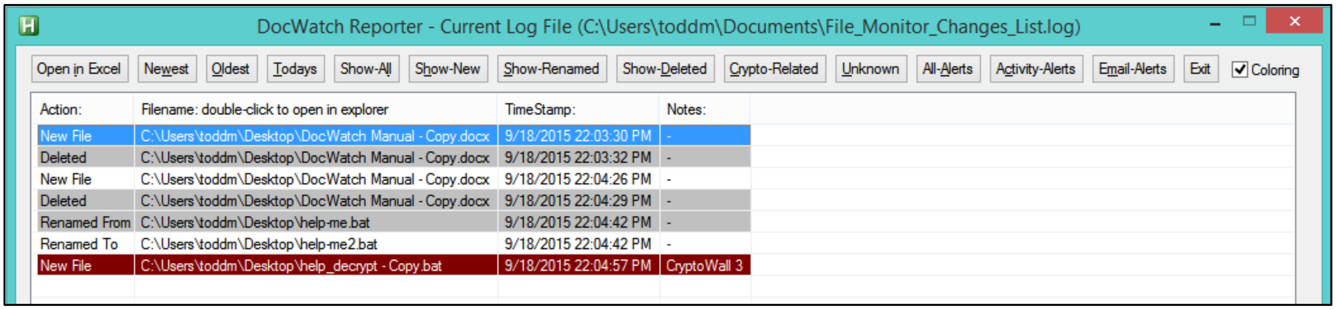

Append to Existing Log

Add changes to the Log file?

Exiting the program:

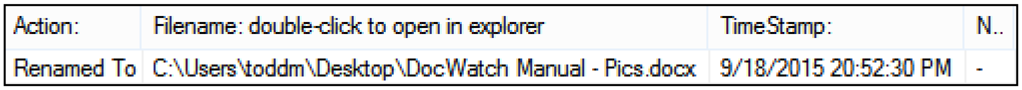
The program may be stopped in two ways. 1) Press Ctrl+F12 to display the Main window then click on the Close button in the upper right corner or 2) Press Shift+Ctrl+F12 to stop the program. This may be done whether the program is visible or hidden.

<u>Display Changes</u> – This option saves in memory changes then displays the current Log file using the DocWatchReport application. Various types of changes are color-coded and there are several buttons that can be used to filter the Log file. The Log file can also be opened up into Excel for those who prefer it.



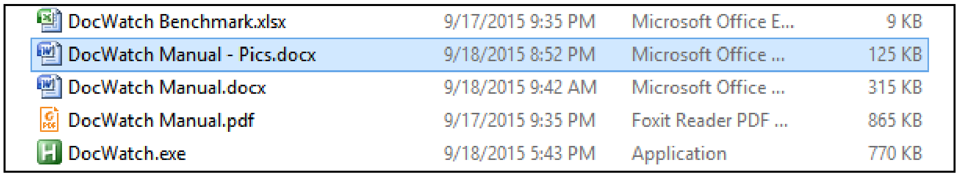
Action:	Filename: double-click to open in explorer	TimeStamp:	Notes:
New File	C:\Users\toddm\Desktop\DocWatch Manual - Copy.docx	9/18/2015 22:03:30 PM	-
Deleted	C:\Users\toddm\Desktop\DocWatch Manual - Copy.docx	9/18/2015 22:03:32 PM	-
New File	C:\Users\toddm\Desktop\DocWatch Manual - Copy.docx	9/18/2015 22:04:26 PM	-
Deleted	C:\Users\toddm\Desktop\DocWatch Manual - Copy.docx	9/18/2015 22:04:29 PM	-
Renamed From	C:\Users\toddm\Desktop\help-me.bat	9/18/2015 22:04:42 PM	-
Renamed To	C:\Users\toddm\Desktop\help-me2.bat	9/18/2015 22:04:42 PM	-
New File	C:\Users\toddm\Desktop\help_decrypt - Copy.bat	9/18/2015 22:04:57 PM	CryptoWall 3

Double-click here:



Action:	Filename: double-click to open in explorer	TimeStamp:	N..
Renamed To	C:\Users\toddm\Desktop\DocWatch Manual - Pics.docx	9/18/2015 20:52:30 PM	-

To browse to the file:

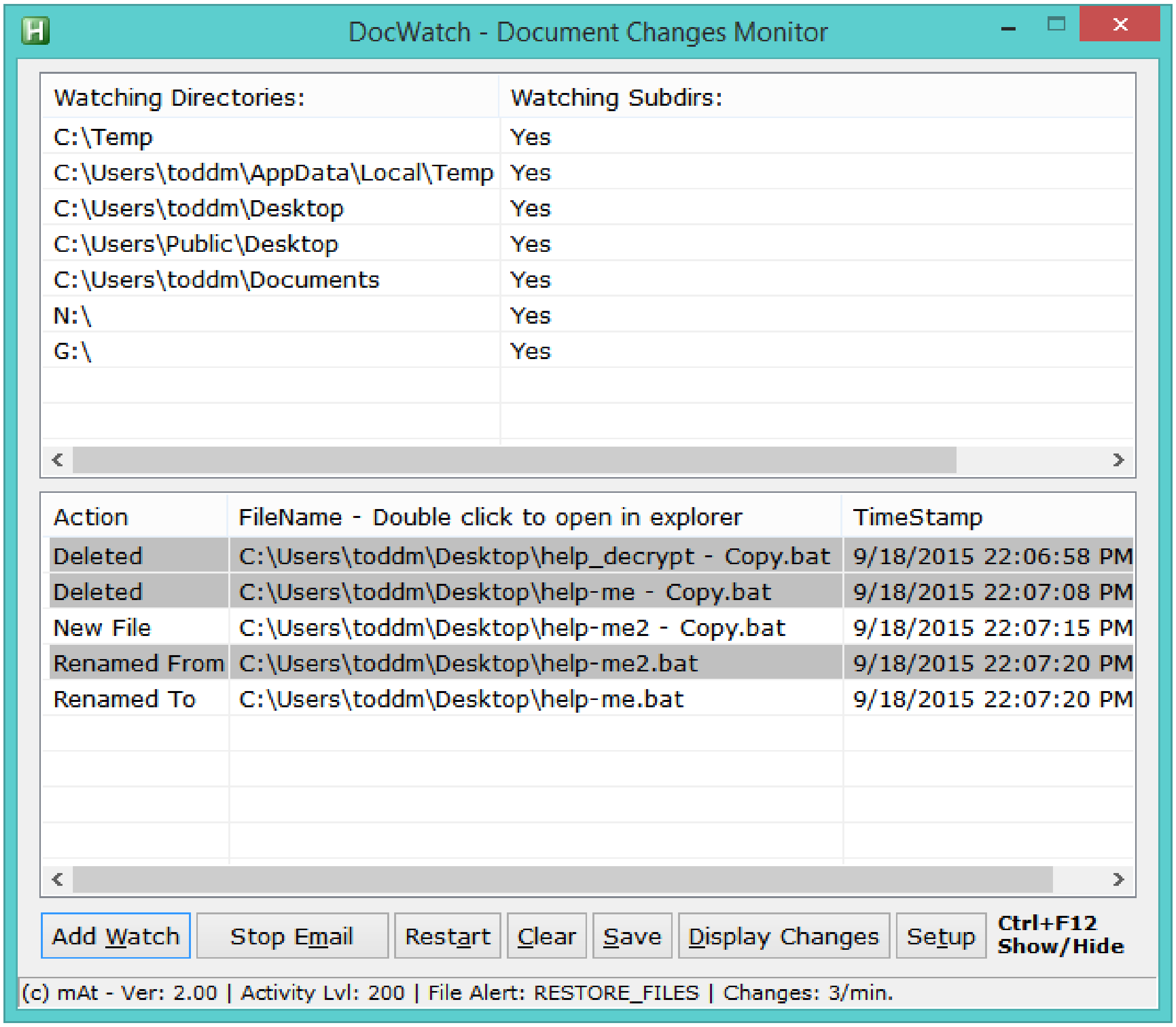


DocWatch Benchmark.xlsx	9/17/2015 9:35 PM	Microsoft Office E...	9 KB
DocWatch Manual - Pics.docx	9/18/2015 8:52 PM	Microsoft Office ...	125 KB
DocWatch Manual.docx	9/18/2015 9:42 AM	Microsoft Office ...	315 KB
DocWatch Manual.pdf	9/17/2015 9:35 PM	Foxit Reader PDF ...	865 KB
DocWatch.exe	9/18/2015 5:43 PM	Application	770 KB

8. <u>Setup</u> – the setup parameters for the program can be displayed/changed at any time with this button.
9. <u>Ctrl+F12</u> – press the Ctrl and F12 keys together to show or hide the Main window. You can also click on the Ctrl+F12 Show/Hide label to hide the Main window.

Extended Version of DocWatch – Using its internal List View:

While it is not recommended for normal usage, due to the fact that the program is actively monitoring files changes on several drives and/or network shares, users can have DocWatch display those changes in real time. As shown below, recent document changes are in the bottom half of the Main window. Users can double-click on a Watch Folder to browse to it. They can also double-click on a changed file to open that folder and highlight the file. Due to the intense nature of monitoring what can be hundreds of file changes per minute, the program will sometimes freeze when the user exits or restarts it.

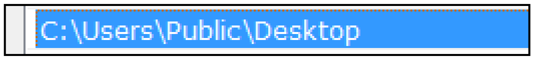


Watching Directories:	Watching Subdirs:
C:\Temp	Yes
C:\Users\toddm\AppData\Local\Temp	Yes
C:\Users\toddm\Desktop	Yes
C:\Users\Public\Desktop	Yes
C:\Users\toddm\Documents	Yes
N:\	Yes
G:\	Yes

Action	FileName - Double click to open in explorer	TimeStamp
Deleted	C:\Users\toddm\Desktop\help_decrypt - Copy.bat	9/18/2015 22:06:58 PM
Deleted	C:\Users\toddm\Desktop\help-me - Copy.bat	9/18/2015 22:07:08 PM
New File	C:\Users\toddm\Desktop\help-me2 - Copy.bat	9/18/2015 22:07:15 PM
Renamed From	C:\Users\toddm\Desktop\help-me2.bat	9/18/2015 22:07:20 PM
Renamed To	C:\Users\toddm\Desktop\help-me.bat	9/18/2015 22:07:20 PM

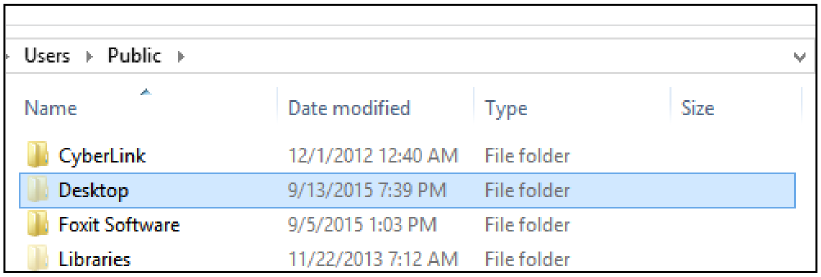
```
(c) mAt - Ver: 2.00 | Activity Lvl: 200 | File Alert: RESTORE_FILES | Changes: 3/min.
```

Double-click here:



C:\Users\Public\Desktop

To see this:



Name	Date modified	Type	Size
CyberLink	12/1/2012 12:40 AM	File folder	
Desktop	9/13/2015 7:39 PM	File folder	
Foxit Software	9/5/2015 1:03 PM	File folder	
Libraries	11/22/2013 7:12 AM	File folder	

Network Files Discussion:

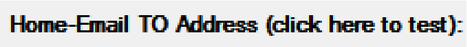
On a network share, the file Owner information can be used and displayed to help verify who created/updated a file. Unfortunately, many times, if John Doe created a file then Jane Smith updates it, the file server will leave the owner as John Doe. If Jane Smith does a copy/paste on the file then the new file will show her as the owner. Even more unfortunate, for Domain Administrators, many files are shown with the owner, BUILT-IN\Administrators, which doesn't help in the determination of who just created or changed files. DocWatch will only break a network connection and shutdown a computer if the created file has a Crypto related filename AND the file owner matches the logged in user on the computer running DocWatch. In any case, DocWatch emails will go out to the address saved in the Setup window.

Files required and created by DocWatch:

- DocWatch.exe (required) – the main executable file contains the files below. It can be run from any directory.
- DocWatchReport.exe (optional) – this program is embedded in the main program and is used to view the currently logged data. It can be launched by clicking on the Display Changes button or run outside the main program. It can be run from any directory. If DocWatch cannot find this program, it will use Notepad instead.
- DocWatch.ini (required) – the information entered into the Setup window is saved to this INI file which is in the same directory as DocWatch.ini.
- DocWatch Manual.pdf (optional) – this instructional guide is embedded in the main program and is displayed by pressing F1 or opening in any PDF viewer. It is placed in the same folder as the main program.
- SwithMail.exe (required) – this program is also embedded in the main program and is extracted to the user's My Documents folder. It is required to create and send email alerts.
- Crypto-Home-Instructions.png (optional) – this is the default PNG drawing for Home users. It contains sample instructions which are displayed after a new Crypto file is detected. Other versions of these instructions can be created with a Paint program to suit the user. It is placed in the C:\Temp folder.
- Crypto-Work-Instructions.png (optional) – this is the same as the prior file but would contain instructions for users in a business environment. Company logo, IT Support information, etc. can be included here. It is placed in the C:\Temp folder.

Quick Guide for end users:

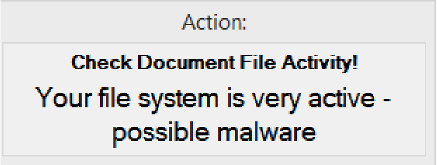
For the average user, they will only need to do the following to get started with the program:

1. Set all the parameters in the Setup window.
2. Test the Home or Work email information by clicking on the Home Email To  Home-Email TO Address (click here to test): and/or the Work Email To bold labels. Depending on your email providers, it may take a couple of minutes for the TEST email to arrive in your Inbox.
3. Click OK to save then exit the Setup window.
4. You will now be at the Main window. If you are satisfied that you have all the needed Watch Folders then you can close the window by pressing the Control and F12 keys (Ctrl+F12) or by clicking at the bottom right of the window where it shows Ctrl+F12 Show/Hide.
5. Now the program is running in the background and actively monitoring document changes.
6. If you want DocWatch to run every time you start your computer then make sure to put a check by ☑ Autostart in the Setup window then click on OK.

Messages and Prompts:

A variety of messages are displayed when either a lot of File Activity or Crypto filenames are found. If List View color is enabled then the colors below will be shown for various changes in the list. Additionally, audio prompts are used.

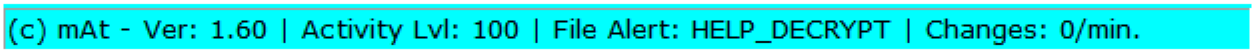
Whenever the Changes per minute Alert value is reached within one minute, a file activity alert is briefly displayed. The color of the status bar will turn Cyan in case the message went unseen.



Action:

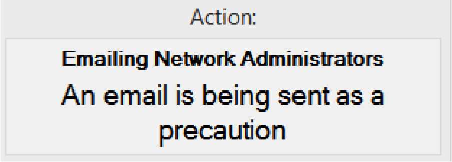
Check Document File Activity!

Your file system is very active - possible malware



(c) mAt - Ver: 1.60 | Activity Lvl: 100 | File Alert: HELP_DECRYPT | Changes: 0/min.

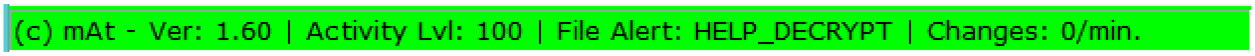
If the same number of files have changed for another two minutes in a row then an email alert is sent out. The color of the status bar will turn Lime in case the message went unseen.



Action:

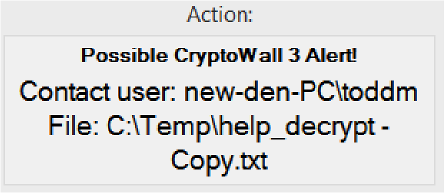
Emailing Network Administrators

An email is being sent as a precaution



(c) mAt - Ver: 1.60 | Activity Lvl: 100 | File Alert: HELP_DECRYPT | Changes: 0/min.

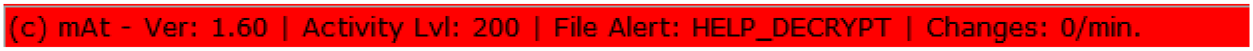
Whenever any file is created or renamed and matches a Crypto related name, the user is prompted with the name of the type of Crypto malware. An email is always sent out for Crypto related files. The status bar is set to Red.



Action:

Possible CryptoWall 3 Alert!

Contact user: new-den-PC\toddm
File: C:\Temp\help_decrypt - Copy.txt

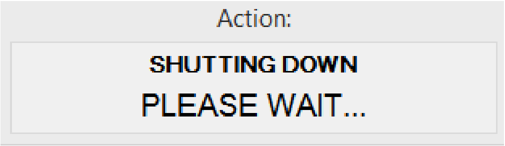


(c) mAt - Ver: 1.60 | Activity Lvl: 200 | File Alert: HELP_DECRYPT | Changes: 0/min.

The program defaults to shutting down the computer when any of the following is true:

- A Crypto related file was created on the local computer hard drive
- A Crypto related file was created on a network drive and its owner name matches the logged in user.

In either of these cases, the user will hear an audio message, an email will be sent and the computer will shutdown. Users should copy/paste sufficient files to simulate Activity Alerts and also create a file called help_decrypy.txt as a test. (Shutdown can be disabled in the Setup window, but, should be left on while learning the program.)

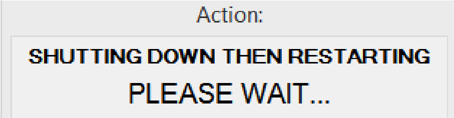


Action:

SHUTTING DOWN

PLEASE WAIT...

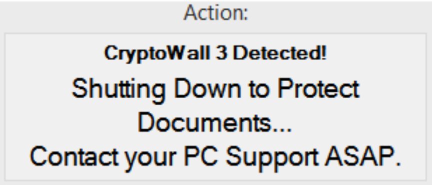
Whenever the Restart button is clicked the following message is briefly shown. This is way to reset the status bar color if needed while not existing the program.


Action:

SHUTTING DOWN THEN RESTARTING

PLEASE WAIT...

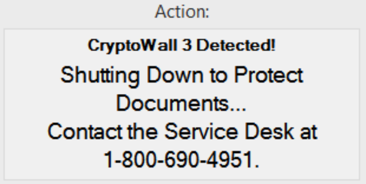
If a Crypto type malware file is detected then it will be displayed with a message to shut down the computer. One message is for home users, the other for office users. The text can be customized in Setup.


Action:

CryptoWall 3 Detected!

Shutting Down to Protect Documents...

Contact your PC Support ASAP.

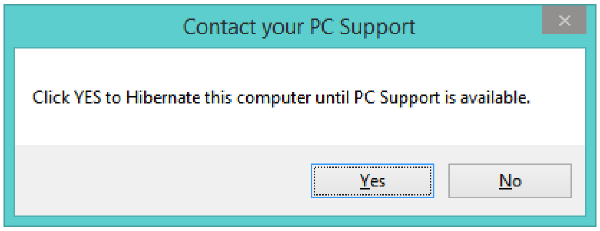

Action:

CryptoWall 3 Detected!

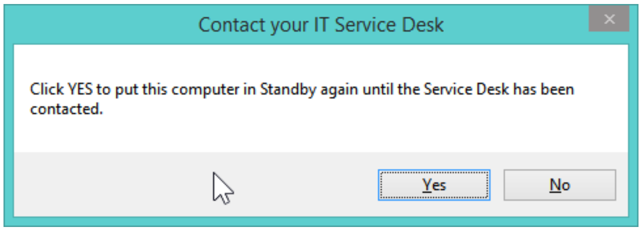
Shutting Down to Protect Documents...

Contact the Service Desk at 1-800-690-4951.

An optional help guide will be display when the computer is powered back on along with the prompt below. It is very important to not leave the computer on or connected to a network when file encryption (damage) may be occurring. So, it is best to shutdown the computer again until you have talked with some Technical Support. You will see the message on the left if at home or the message on the right if you in an office environment.


Contact your PC Support

Click YES to Hibernate this computer until PC Support is available.


Contact your IT Service Desk

Click YES to put this computer in Standby again until the Service Desk has been contacted.

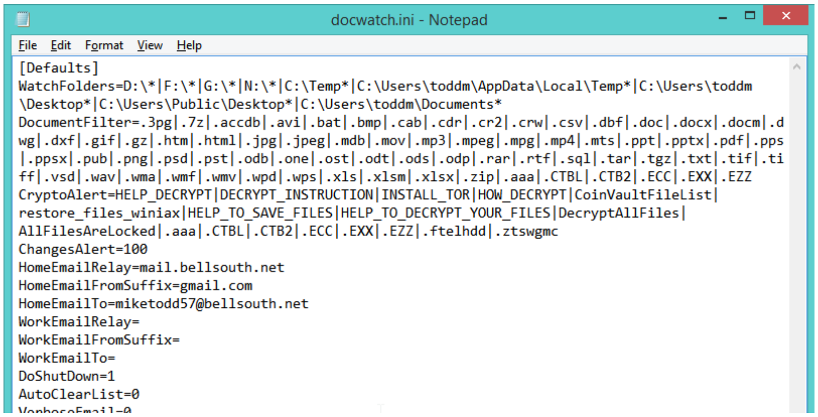
Keyboard Commands:

The following two options are available through keyboard shortcuts –

F1 – displays this Users Guide	Ctrl+F12 – pressing both Ctrl and F12 will either display the Main Window or hide it
Shift+Ctrl+F12 – pressing Shift plus Ctrl and F12 will terminate the program. It is the same as clicking on the Red X in the upper right of the window ✕.	Ctrl+F9 – displays the current Log file in DocWatchReport. Users may use this key combination even when the Main window is hidden.

DocWatch.ini file:

Whenever the Setup window is display then closed by clicking OK, a settings file is created in the same folder as the program. It is called DocWatch.ini and looks like the following.

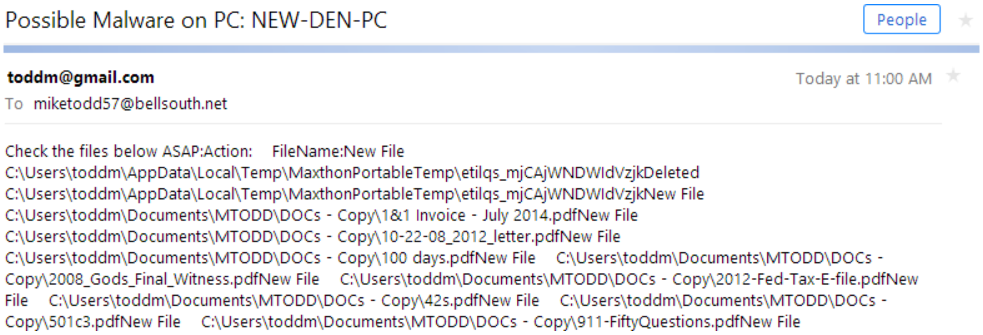


```
[Defaults]
WatchFolders=D:\*|F:\*|G:\*|N:\*|C:\Temp*|C:\Users\toddm\AppData\Local\Temp*|C:\Users\toddm
\Desktop*|C:\Users\Public\Desktop*|C:\Users\toddm\Documents*
DocumentFilter=.3pg|.7z|.accdb|.avi|.bat|.bmp|.cab|.cdr|.cr2|.crw|.csv|.dbf|.doc|.docx|.docm|.d
wg|.dxf|.gif|.gz|.htm|.html|.jpg|.jpeg|.mdb|.mov|.mp3|.mpeg|.mpg|.mp4|.mts|.ppt|.pptx|.pdf|.pps
|.ppsx|.pub|.png|.psd|.pst|.odb|.one|.ost|.odt|.ods|.odp|.rar|.rtf|.sql|.tar|.tgz|.txt|.tif|.ti
ff|.vsd|.wav|.wma|.wmf|.wmv|.wpd|.wps|.xls|.xlsm|.xlsx|.zip|.aaa|.CTBL|.CTB2|.ECC|.EXX|.EZZ
CryptoAlert=HELP_DECRYPT|DECRYPT_INSTRUCTION|INSTALL_TOR|HOW_DECRYPT|CoinVaultFileList|
restore_files_winiax|HELP_TO_SAVE_FILES|HELP_TO_DECRYPT_YOUR_FILES|DecryptAllFiles|
AllFilesAreLocked|.aaa|.CTBL|.CTB2|.ECC|.EXX|.EZZ|.ftelhdd|.ztswgmc
ChangesAlert=100
HomeEmailRelay=mail.bellsouth.net
HomeEmailFromSuffix=gmail.com
HomeEmailTo=miketodd57@bellsouth.net
WorkEmailRelay=
WorkEmailFromSuffix=
WorkEmailTo=
DoShutDown=1
AutoClearList=0
VerboseEmail=0
```

Email Alerts:

There are two types of email alerts the program can generate, one is after excessive file activity and the other is for Crypto filenames being detected. Typical subject lines are shown below. The computer name and last scanned filename are included.

1. Possible Malware

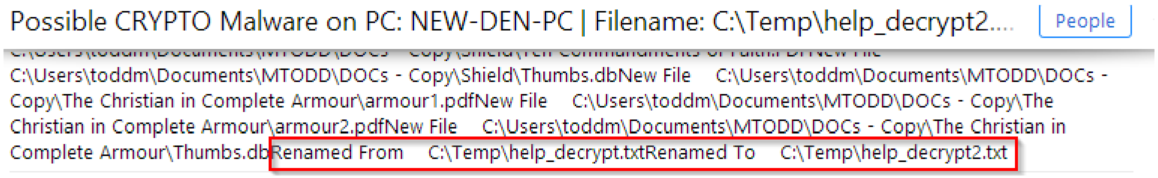


Possible Malware on PC: NEW-DEN-PC

toddm@gmail.com
To miketodd57@bellsouth.net
Today at 11:00 AM

Check the files below ASAP:Action: FileName:New File C:\Users\toddm\AppData\Local\Temp\MaxthonPortableTemp\etilqs_mjCAjWNDWIdVzjkDeleted C:\Users\toddm\AppData\Local\Temp\MaxthonPortableTemp\etilqs_mjCAjWNDWIdVzjkNew File C:\Users\toddm\Documents\MTODD\DOCs - Copy\1&1 Invoice - July 2014.pdfNew File C:\Users\toddm\Documents\MTODD\DOCs - Copy\10-22-08_2012_letter.pdfNew File C:\Users\toddm\Documents\MTODD\DOCs - Copy\100 days.pdfNew File C:\Users\toddm\Documents\MTODD\DOCs - Copy\2008_Gods_Final_Witness.pdfNew File C:\Users\toddm\Documents\MTODD\DOCs - Copy\2012-Fed-Tax-E-file.pdfNew File C:\Users\toddm\Documents\MTODD\DOCs - Copy\42s.pdfNew File C:\Users\toddm\Documents\MTODD\DOCs - Copy\501c3.pdfNew File C:\Users\toddm\Documents\MTODD\DOCs - Copy\911-FiftyQuestions.pdfNew File

2. Possible CRYPTO Malware



Possible CRYPTO Malware on PC: NEW-DEN-PC | Filename: C:\Temp\help_decrypt2....

C:\Users\toddm\Documents\MTODD\DOCs - Copy\Shield\Thumbs.dbNew File C:\Users\toddm\Documents\MTODD\DOCs - Copy\The Christian in Complete Armour\armour1.pdfNew File C:\Users\toddm\Documents\MTODD\DOCs - Copy\The Christian in Complete Armour\armour2.pdfNew File C:\Users\toddm\Documents\MTODD\DOCs - Copy\The Christian in Complete Armour\Thumbs.dbRenamed From C:\Temp\help_decrypt.txtRenamed To C:\Temp\help_decrypt2.txt

Crypto Malware Info:

Activities of the following malwares are currently detected –

Malware name:	Associated Files:
CryptoWall 3	HELP_DECRYPT
CryptoWall 2	DECRYPT_INSTRUCTION, INSTALL_TOR
CTB Locker	AllFilesAreLocked, DecryptAllFiles, .CTBL and .CTB2 file extensions
HOW Decrypt Ransomware	HOW_DECRYPT
Coin Vault	CoinVaultFileList
CryptoWall variants	restore_files_winiax, .aaa file extensions
TeslaCrypt	HELP_TO_SAVE_FILES, HELP_TO_DECRYPT_YOUR_FILES, .ECC and .EXX file extensions
AlphaCrypt	.EZZ file extension
TeslaCrypt newer	RESTORE_FILES_random.txt and .ABC extensions

These malware filenames can be updated as need in the Setup window.