

# Ransomware Detection Service

## Main Description:

This program detects all present and future ransomware in Windows file shares or local drives.

This program helps to detect when/where ransomware has hit Windows file shares or local drives. This program doesn't prevent ransomware infection. Go to <http://www.questiondriven.com/2016/03/07/how-to-prevent-ransomware-infections/> for prevention recommendations.

When staff members get ransomware, you need to respond quickly to get their computer shutdown as soon as possible. If you respond quickly enough, you can shut down the offending computer before other file shares become encrypted. Anti-virus programs currently do not detect encrypted files written by ransomware. Not knowing that a ransomware virus is on your network is a big problem. The sooner you get the offending computer shutdown and restore your backups of files shares the better.

File servers do not get the virus, the virus encrypts the files stored on the file server. This makes knowing the damage caused by a ransomware difficult. If you do not notice an encrypted file share, you can lose your opportunity to restore from backup or cause your users to use a much older backup than necessary. Anti-virus programs are always a few days behind in detecting new viruses.

I added the ability to Find Ransomware Files (during off hours) to help determine damage caused by a previous uncaught infection. I just added the ability to delete any ransomware created files for cleanup purposes after you restore your files from backup. To get a listing of files that were encrypted use the Find Ransomware Files tab.

## Caveat:

- Train or notify users to not delete the files/folders that are copied from the SourcePath. Deleted files will cause a false positive missing files error message or email.
- If you are using the important files method then you will receive error messages for all changed files (even when changed normally).
- Find Ransomware Files tab will be slow for large directories with many files. Only run this during off hours. Run Compare (Detection Ransomware) during business hours if you use small example source files.

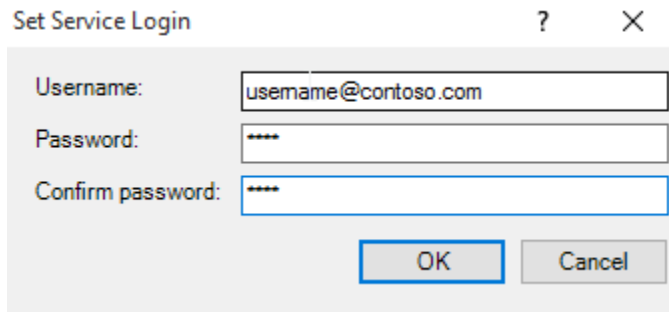
## System Requirements:

- Windows Server 2008 or newer or Windows 7 or newer and both 32 bit and 64 bit OS's are supported
- At least .Net 4.0

## Installation:

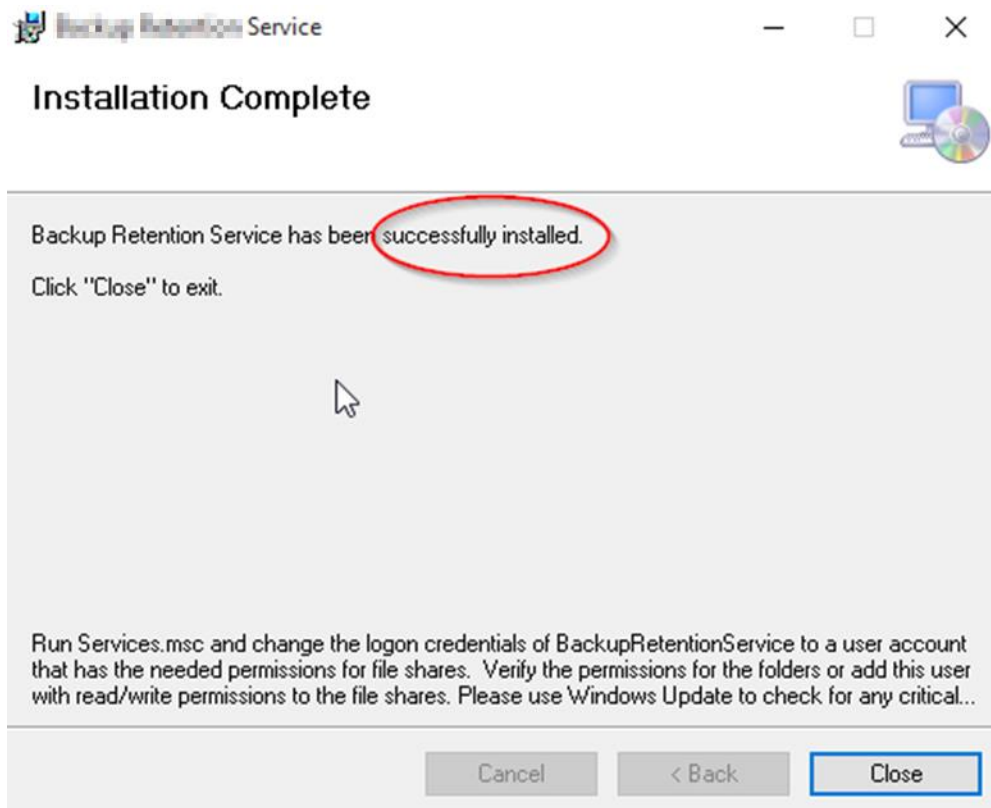
1. Download both Installer Files (setup.exe and RansomwareDetectionServiceInstaller.msi) into the same directory and run setup.exe as administrator <http://ransomwaredetectionservice.codeplex.com>

2. Run the installation setup.exe downloaded from step 1 (Username for the service will be requested before installing the Windows service (username must to be in "username@contoso.com" format.)
3. Beta Test Article: <http://www.questiondriven.com/2016/02/18/beta-testing-for-ransomware-detection-in-file-share/> and beta test discussion page on codeplex <https://ransomware detectionservice.codeplex.com/discussions>



A dialog box titled "Set Service Login" with a question mark icon and a close button (X). It contains three input fields: "Username:" with the text "username@contoso.com", "Password:" with four asterisks, and "Confirm password:" with four asterisks. At the bottom are "OK" and "Cancel" buttons.

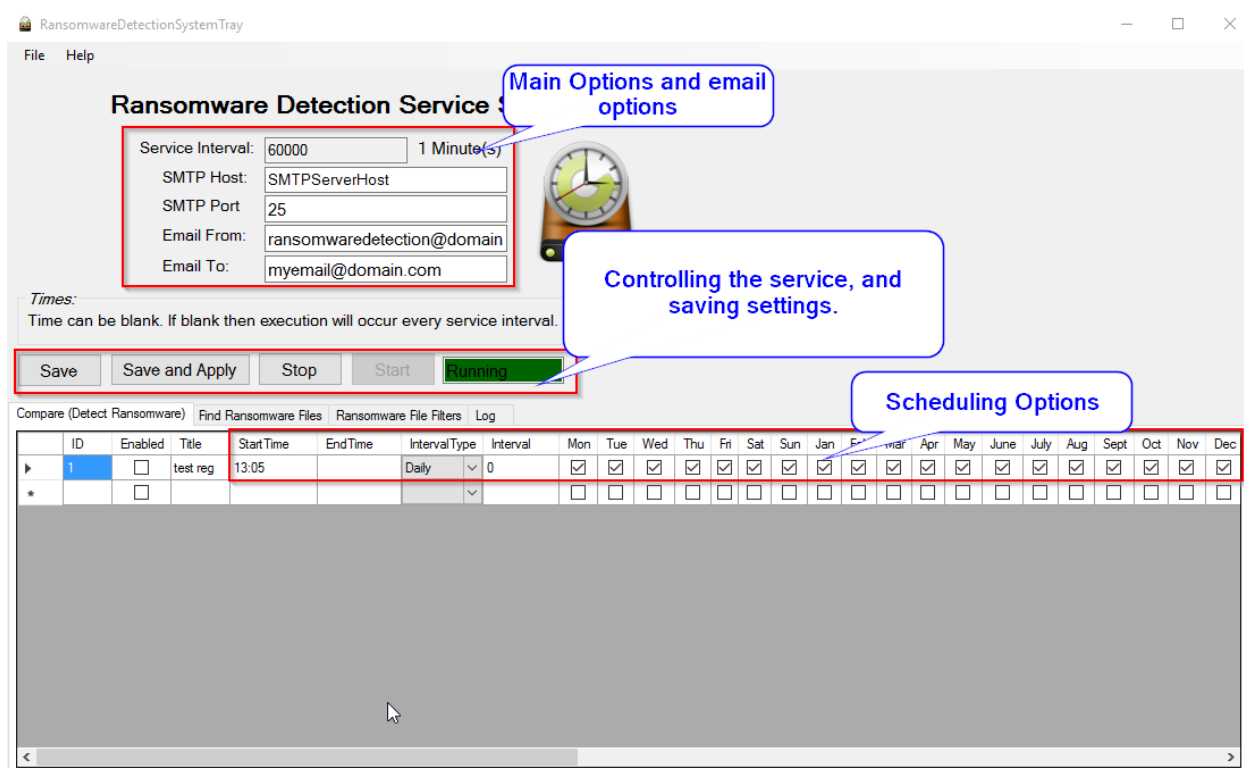
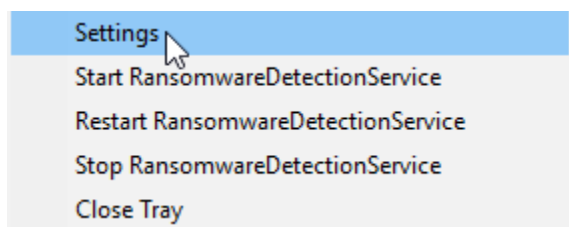
If you specified the username correctly and clicked on OK, then the install will show success. This domain username will need at least read access to the files shares you want to monitor. The copy options require read/write access to the file share.



After install launch the system tray application then right click on it. (You might have to click on the little arrow on the left of the system tray to show hidden system tray icons)



You will see the following options (click on settings to display the main form for changing settings):



RansomwareDetectionSystemTray

File Help

## Ransomware Detection Service Settings

Service Interval:  2 Minute(s)

SMTP Host:

SMTP Port:

Email From:

Email To:

**Times:**  
Time can be blank. If blank then execution will occur every service interval

Compare (Detect Ransomware) Log

SourcePath	FilePathToCheck	CheckMainFolder	CheckSubFolders	CopySourceFiles	CopySourceFilesSubFolders	SendEmailOnFailure	SendEmailOnSuccess
C:\TEMP\source	C:\TEMP\filestocheck	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

After Scheduling options to the right there are specific options for the tab selected

### Installation and Use Notes:

- I created the ability to detect ransomware in file shares using the Compare tab.
- RansomwareDetectionService is a C# Windows service that will detect ransomware in a windows file share and optionally copy the files you want to verify to the SourcePath and the first layer of subfolders as well.
- Run services.msc and changed the logon user and password for "RansomwareDetectionService" to the user that has the needed permissions for the folders you are working with.
- Make sure to use UNC paths for file shares or a local folder for the Windows Server running the service.

### Overall Features:

- SourcePath files and folders are checked against the FilePathToCheck and if files are changed or missing then an error is logged and an email sent if SendEmailOnError is checked.
- Each row in the configuration table can run on a different schedule and have different options.
- Long path names are supported.
- Configuration table rows are executed via a multi-threaded call. Therefore, multiple folders can be scheduled to be checked and even run at the same time.

### Scheduling Options:

- Time Based or Interval Based Execution for each item in each configuration table.
- Day of the Week Selection via check box for Monday - Sunday
- Day of the Month Enter in day 1-31 desired and this will override Day of the Week
- Day of the Month Enter in -1 to -5 for NthDayOfTheWeek (where -1 is 1st day of the month and -5 is 5th day in the month) in conjunction with Day of the Week to select the desired WeekDay.
- Each configuration runs on a different thread so that they can run at the same time if needed and you don't see a file locking problem possible.
- **Interval Type:**

- Hourly: Enter start time in military time, end time in military time, select hourly interval type, and enter "interval" in minutes.
- Daily: Set a start time in military format, select days and months you want to run and it will run at that time.
- Monthly: Set Interval to 1-31 to run on a specific day of the month, specify -1 up to -5 and select a day to set the nth day of the month (e.g. -1 Mon would run on the 1st Monday of the month.)

## Example Hourly and Daily Schedules:

Compare (Detect Ransomware)					Find Ransomware Files (Off Hours Only)					Ransomware File Filters					Log												
	StartTime	EndTime	IntervalType	Interval	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec				
Hourly Example Schedules	06:00	23:59	Hourly	30																							
	06:00	23:59	Hourly	23																							
	06:00	23:59	Hourly	27																							
	06:00	23:59	Hourly	33																							
	06:00	23:59	Hourly	37																							
	06:00	23:59	Hourly	43																							
	06:00	23:59	Hourly	45																							
	05:05		Daily	0																							
Some Daily Example Schedules	05:07		Daily	0																							
	05:10		Daily	0																							
	05:13		Daily	0																							
	05:16		Daily	0																							
	05:20		Daily	0																							
	05:25		Daily	0																							
	05:30		Daily	0																							

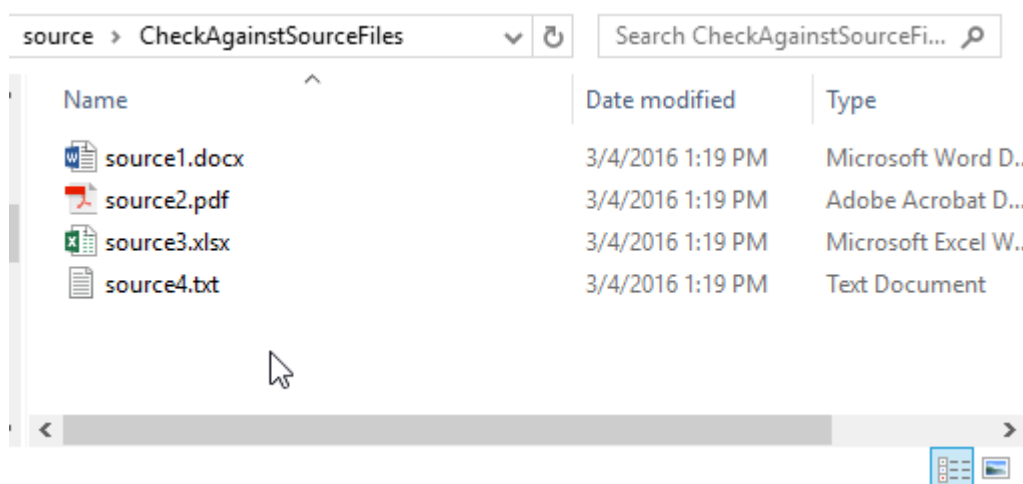
## Compare (Detect Ransomware in file share) Explanation and Overall Features:

Copy source files into the file path to check and then on a schedule check to see if the source files have changed or went missing. There are two ways to test for ransomware. First, create a folder in the SourcePath with a few small files with files of the type that you are concerned (XLS, XLSX, DOC, DOCX, PDF, JPG, PNG, TXT, etc.). Copy this directory to each folder that you want to monitor or use CopySourceFiles or CopySourceFilesSubFolders options in order to copy the SourcePath files (only needs to run once with these options). If these files change or get encrypted then you will receive an error in the error log and possibly an email if setup. Secondly you could put a copy of important files into the SourcePath and have it monitoring for changes (This will take longer but you will know when important files are changed)

SourceFiles: Source Folder with a few example files that will copy and compare later. Make sure this path is not shared.

## Example Options (Entrapment):

Example Files for Comparison Later:



Immediate sub folders are compared but not the main folder, SourcePath folders and files are copied; If they go missing an error is logged/emailed and the files are copied again. FilePathToCheck should be a windows file share, but SourcePath should not be a file share.

Compare (Detect Ransomware) Find Ransomware Files (Off Hours Only) Ransomware File Filters Log							
	SourcePath	FilePathToCheck	CheckMainFolder	CheckSubFolders	ExcludeFolders	CopySourceFiles	CopySourceFilesSubFolders
▶	C:\TEMP\source	C:\TEMP\filestocheck	<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>
*			<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>

### Compare Options:

- **SourcePath:** Folder where files that will be used as the source for comparison (A file path that cannot be reached via a file share, and non-admin users do not have rights to modify are recommended.) I recommend creating a few simple files with extensions you care to monitor. These files will be copied to your FilePathToCheck Main folder for immediate sub folders and if these files are modified or the files are missing, then you can be notified of the problem.
- **FilePathToCheck:** This is the file share that you want to monitor for ransomware or monitor the files for changes
- **CheckMainFolder:** Check the main FilePathToCheck to see if it has the SourcePath files exist in FilePathToCheck directory and are not changed.
- **CheckSubFolders:** Check the immediate sub folders of FilePathToCheck to see if it has the SourcePath files exist in each sub folder of the FilePathToCheck directory and are not changed.
- **CopySourceFiles:** Copies SourcePath files to FilePathToCheck if the files do not exist (This will make the "Files Missing" error only fire once.)
- **CopySourceFilesSubFolders:** Copies SourcePath files to each immediate sub folder of FilePathToCheck if the files do not exist. (This will make the "Files Missing" error only fire once). I recommend that you only run this option once and then turn off on subsequent runs.

- **SendEmailOnFailure:** Sends summary email when files are changed or if files are missing each time the directory is compared.
- **SendEmailOnSuccess:** Sends summary email notifying you that the file path was checked.
- **ExcludedFolders:** Excludes list of folders separated by semicolon from the immediate sub folder check and immediate sub folder copy as well.

## **Find Ransomware Files (Search for Ransomware created files)**

The “Find Ransomware Files” tab searches all the specified directories for the ransomware file filters that you specify in the “Ransomware File Filters” tab. This solves the following two problems.

- Files screens will detect files new files modified or created by old ransomware, but how do you find ransomware files that already exist. How do you detect where the new ransomware hit your file shares? How do you find ransomware files with folder or file names with long path names? How do you remove ransomware created files after you restore from backup?

### **Find Ransomware Files Options:**

- **FilePathToCheck:** This is the file share that you want to monitor for ransomware or monitor the files for changes
- **CheckSubFolders:** Recursively check all the sub folders of FilePathToCheck.
- **SendEmailOnFailure:** Sends summary email when files are changed or if files are missing each time the directory is compared.
- **SendEmailOnSuccess:** Sends summary email notifying you that the file path was checked.
- **ExcludedFolders:** Excludes list of folders separated by semicolon from FilePathToCheck. Any folder matching the exact name will be excluded.
- **Ransomware File Filters (tab)**
  - **Enabled:** Search for this FileFilter
  - **Title:** Name of ransomware to find or description of search
  - **FileFilter:** Enter in file filter search expected by windows (e.g. \*recover\*.txt, HELP\_RESTORE\_FILES.txt, or \*.ecc)
  - **ExcludeFiles:** Semicolon separated list of exact files names to exclude from results and delete. List false positive files found from a previous run of Find Files.
  - **ObjectType:** Search for File, Folder or Both.
  - **DeleteFilesFound:** Delete all files found by the file filter. (Only check mark this after you have verified the files you want to delete by a previous run and no false positives will be deleted. Uncheck this after it has run once. I recommend using a very specific file filter with this option.)
  - **Comment:** a comment regarding the file filter

## Find Ransomware Files (Off Hours Only) tab:

RansomwareDetectionSystemTray

File Help

### Ransomware Detection Service Settings

Service Interval: 60000 1 Minute(s)

SMTP Host: SMTPServer

SMTP Port: 25

☐ SMTP Use SSL

☒ SMTP Use Default Credentials

SMTP Username:

SMTP Password:

Email From: rdetect@emaildomain.com

Email To: test@emaildomain.com

Send Test Email

Service Status: Running

Save Save and Apply Stop Start

Compare (Detect Ransomware) Find Ransomware Files (Off Hours Only) Ransomware File Filters Log

FilePathToCheck	CheckSubFolders	ExcludeFolders	SendEmailOnFailure	SendEmailOnSuccess	StartDate	EndDate
c:\users\Documents	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3/1/2016	

## File Filters tab (More filters can be added at any time):

Compare (Detect Ransomware) Find Ransomware Files (Off Hours Only) Ransomware File Filters Log									
	ID	Enabled	Title	FileFilter	ExcludeFiles	ObjectType	DeleteFilesFound	Comment	
▶	1	<input checked="" type="checkbox"/>		*.0x0		File	<input type="checkbox"/>		
	2	<input checked="" type="checkbox"/>		*.1999		File	<input type="checkbox"/>		
	3	<input checked="" type="checkbox"/>		*.73i87A		File	<input type="checkbox"/>		
	4	<input checked="" type="checkbox"/>		*.7z.encrypted		File	<input type="checkbox"/>		
	5	<input checked="" type="checkbox"/>		*.aaa		File	<input type="checkbox"/>		
	6	<input checked="" type="checkbox"/>		*.abc		File	<input type="checkbox"/>		
	7	<input checked="" type="checkbox"/>		*.bleep		File	<input type="checkbox"/>		
	8	<input checked="" type="checkbox"/>		*.ccc		File	<input type="checkbox"/>		
	9	<input checked="" type="checkbox"/>		*.cerber		File	<input type="checkbox"/>		
	10	<input checked="" type="checkbox"/>		*.crinf		File	<input type="checkbox"/>		
	11	<input checked="" type="checkbox"/>		*.crjoker		File	<input type="checkbox"/>		
	12	<input checked="" type="checkbox"/>		*.crypt		File	<input type="checkbox"/>		
	13	<input checked="" type="checkbox"/>		*.crypto		File	<input type="checkbox"/>		



## Audit Files (Search for Ransomware Affected Files)

If a ransomware file changes files in your files shares it is important to know the extent of the damage caused by the virus. The “Audit Files” tab will search specified directories and compare the file header/signature vs known file headers for the file extension. If a compared file does not match the header is outputted into the UnverifiedFiles.csv file. If a file extension is not known then the file is outputted into the UnknownFiles.csv file. Files that match the known file header/signature will output into the VerifiedFiles.csv file.

Compare (Detect Ransomware)	Find Ransom Files (Off Hours Only)	Find Filters	Audit Files (Off Hours Only)	Audit Signatures	Log			
	FilePathToCheck	CheckSubFolders	ExcludeFolders	ExportCSVPath	ExportUnVerifiedToCSV	ExportVerifiedToCSV	ExportUnknownToCSV	ExportProhibitedToC
▶	C:\TEMP\filestochek	<input checked="" type="checkbox"/>		C:\TEMP\ExportCSV	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
*		<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Audit Files Options:

- **FilePathToCheck:** This is the file share that you want to monitor for ransomware or monitor the files for changes
- **CheckSubFolders:** Recursively check all the sub folders of FilePathToCheck.
- **ExcludedFolders:** Excludes list of folders separated by semicolon from FilePathToCheck. Any folder matching the exact name will be excluded.
- **ExportCSVPath:** The path where the csv files will be saved (UnknownFiles.csv, UnVerifiedFiles.csv, and VerifiedFiles.csv)
- **ExportUnVerifiedToCSV:** Saves unverified (Possible ransomware affected files) to csv file
- **ExportVerifiedToCSV:** Saves file header verified list of files to csv file. (Prohibited files will also be in this list if the signature matches the file extension)
- **ExportUnknownToCSV:** Saves unknown (extension is unknown or error on reading the file) list of files to csv file.
- **ExportProhibitedToCSV:** If any signatures and extensions are flagged as prohibited then they will be added to the prohibited csv file.
- **SendEmailOnFailure:** Sends summary email of files that were possibly affected by ransomware.
- **SendEmailOnSuccess:** Sends summary email notifying you that the file path was audited.
- **Audit Signatures tab** (If no signatures are listed then the stock signatures are used)
  - **Enabled:** Whether signature check is enabled
  - **ByteOffset:** Number of bytes to ignore previous to the Hexadecimal Pattern.
  - **HexPattern:** The hexadecimal pattern to find within the first 100 bytes of a file.
  - **SignaturesName:** The file type title or signature name
  - **FileExtensions:** a semicolon separated list of file extensions to match with the signatures include the period with each file extension e.g. .doc;.docx;xls;xlsx
  - **Prohibited:** If prohibited then any file with the extension and signature will be added to the prohibited list. The file will also be listed in the verified list if signature hexadecimal pattern matches the file extension.
  - **Comment:** A comment for the signature.

**BSD License:**

Copyright (c) 2016, Preston Cooper – HESD Ransomware Detection Service

<http://www.questiondriven.com>

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## **Delimon.Win32.IO Class License:**

Copyright © 2012, Johan Delimon

<http://bit.ly/delimon>

All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.

IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.