Ransomware Detection Service

Main Description:

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

This program doesn't prevent ransomware infection. This program helps to detect when/where ransomware has hit Windows file shares or local drives.

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 search (during off hours) for ransomware specific files 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 an infection to a file share. Make note of the owner of ransomware created files and date/time created before deletion. Run the search with deletion option unchecked at least once to verify find file results so that unexpected files are not deleted. Searching long path file/folder names and hidden files/folders are supported.

Caveat:

- Train or notify users to not delete the files/folders that get 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 for large directories with many files will be slow and should be run during off hours. Compare (Detect Ransomware) is fast and can be run during business hours.
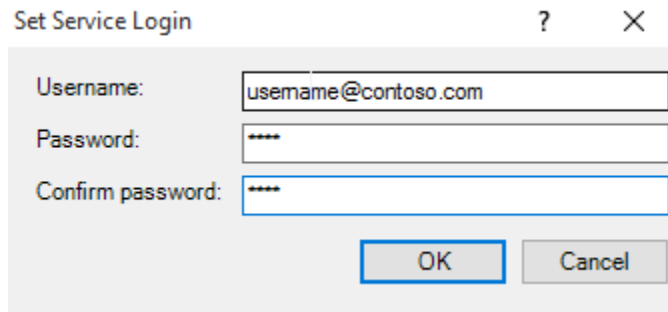
System Requirements:

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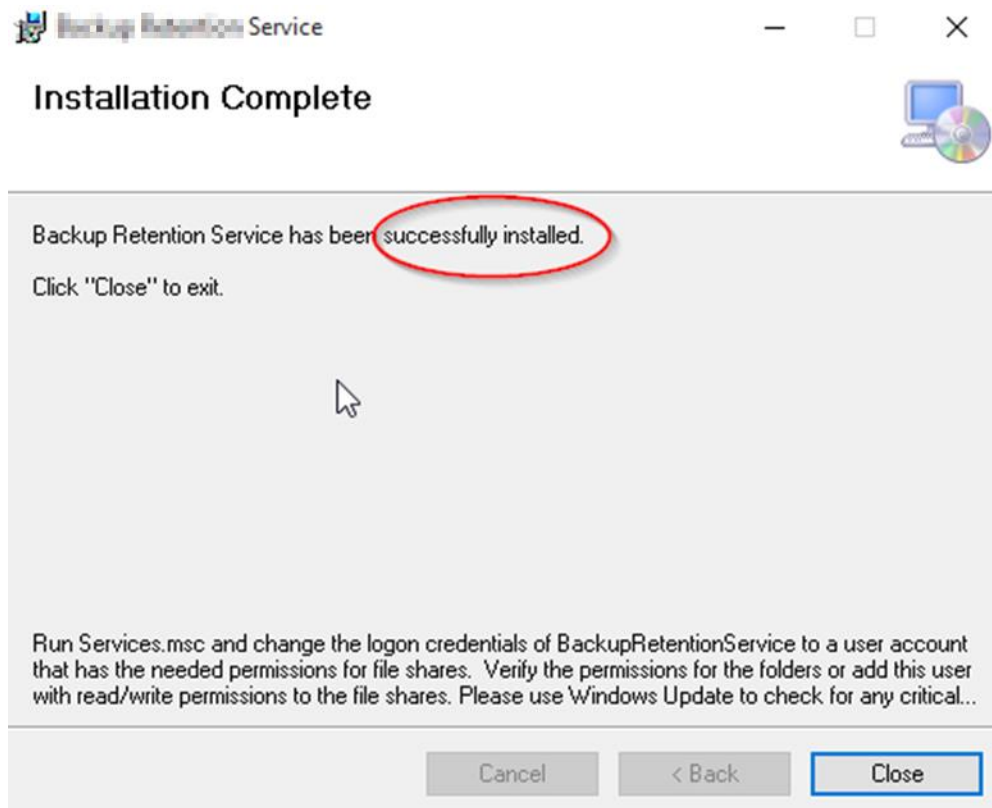- At least .Net 4.0

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.)

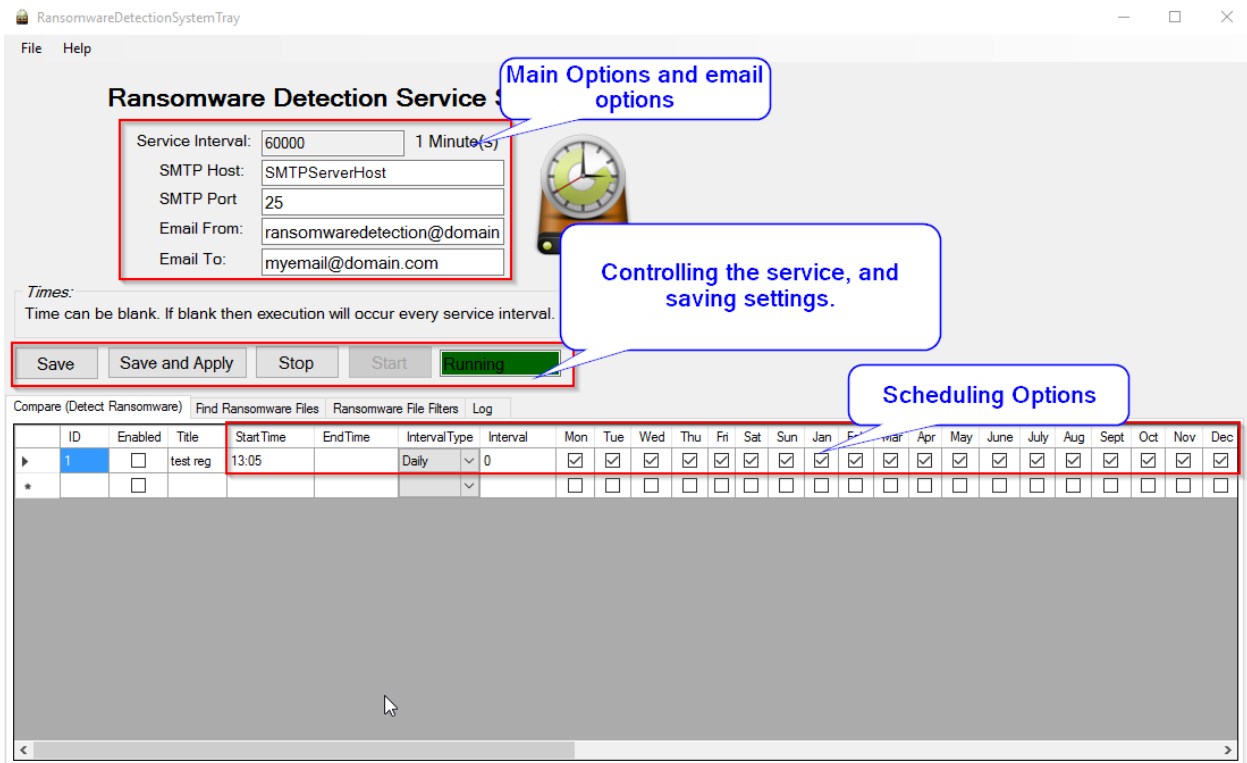3. Beta Test Article: http://www.questiondriven.com/2016/02/18/beta-testing-for-ransomware-detection-in-file-share/ and beta test discussion page on codeplex https://ransomwaredetectionservice.codeplex.com/discussions

If you specified the username correctly and clicked on OK, then the install will show success. This is the domain username that will need at least read access to the files shares you want to monitor. To use the copy options read/write access is needed.

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):

Settings
Start RansomwareDetectionService
Restart RansomwareDetectionService
Stop RansomwareDetectionService
Close Tray

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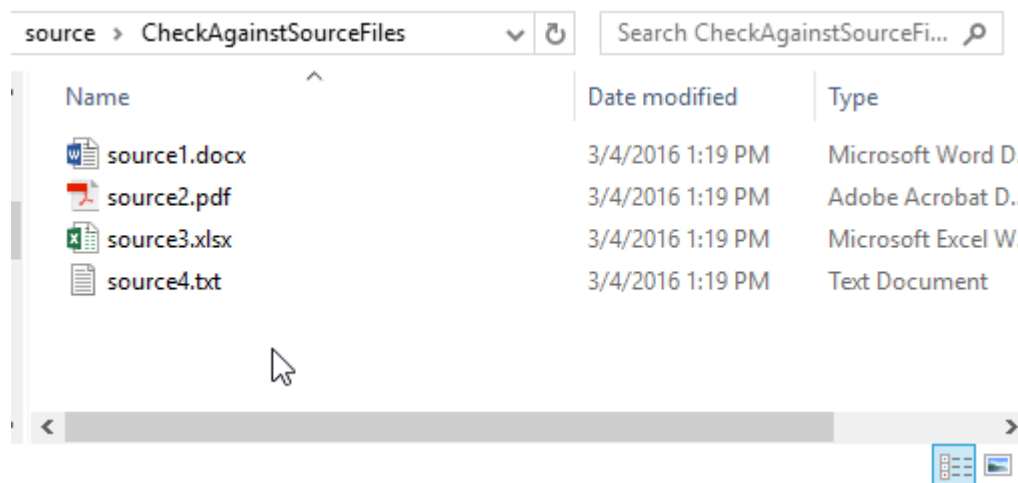
Immediate sub folders are compared but not the main folder, SourcePath folders and files are copied; If they go missing an error is logged/emailed and the files are copied again. FilePathToCheck should be a windows file share, but SourcePath should not be a file share.

Compare 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 is 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 is 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 subsequence 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)
    - o Enabled: Search for this FileFilter
    - o Title: Name of ransomware to find or description of search
    - o FileFilter: Enter in file filter search expected by windows (e.g. *recover*.txt, HELP_RESTORE_FILES.txt, or *.ecc)
    - o 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.
    - o 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.)
- o   Comment: a comment regarding the file filter

Find Ransomware Files (Off Hours Only) tab:

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

Delimon.Win32.IO Class License: