Setup Guide for Server Ransomware Protection

This document will give examples of how to setup monitors to protect against ransomware using a variety of techniques.

In the examples below, we'll assume we're protecting the D:\ drive.

There are two parts to the document: Detection Methods, and Protection Responses.

Detection Methods

There are three methods for detecting ransomware:

1. Heuristics – detect the pattern that ransomware has to use (read the file, write it back in an encrypted format, and then delete the original file). This is the most reliable option.

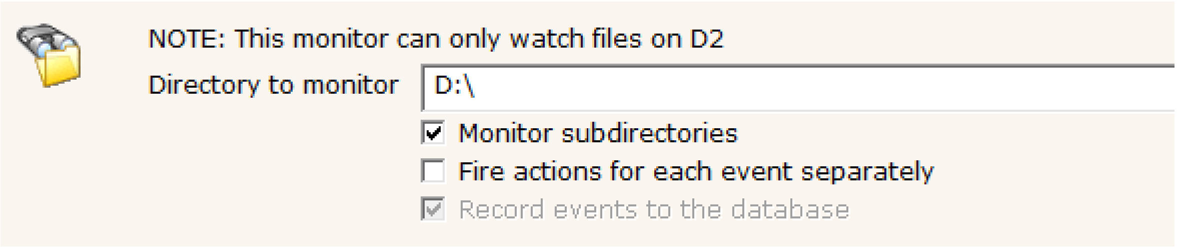
2. Honeypots – create a folder that users should never access, and if it is accessed, assume it is software misbehaving (ransomware)

3. Well known file extensions and filenames – people on the Internet have been keeping lists of how filenames are changed when files are encrypted, and PA File Sight can watch for those specific lists.

Detection via Heuristics

This is PA File Sight's strongest detection method. It requires a feature that is only available in the Ultra edition of the product (the User Activities tab).

To set it up, create a new File Sight monitor, and enter the path to monitor, as shown below:



NOTE: This monitor can only watch files on D2

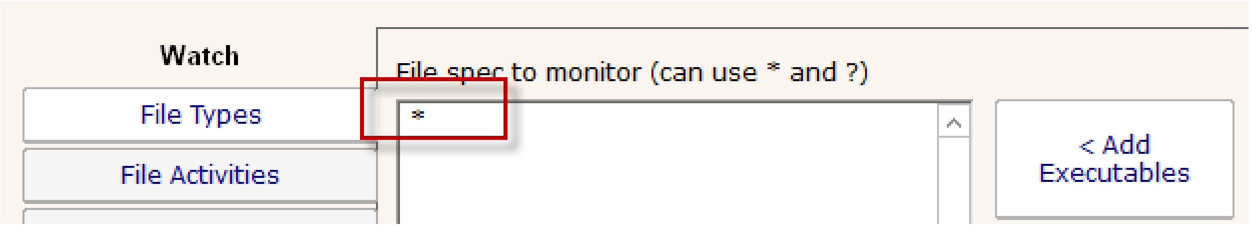
Directory to monitor: D:\

☑ Monitor subdirectories

☐ Fire actions for each event separately

☑ Record events to the database

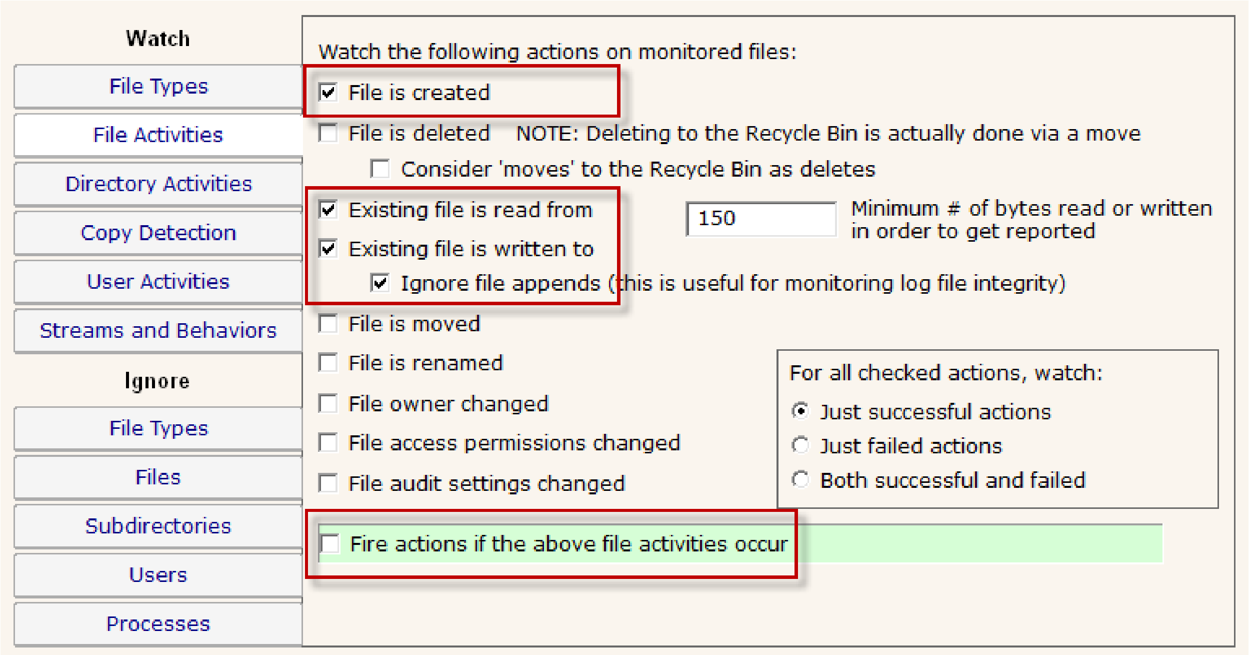
Leave the File Types tab with the default of monitoring all files as shown:



File spec to monitor (can use * and ?)

*

On the File Activities tab, only watch file Creates, Reads and Writes as shown below. Be sure to uncheck the green box – you don't want to fire alerts for all file reads and writes.



Watch the following actions on monitored files:

☑ File is created

□ File is deleted   NOTE: Deleting to the Recycle Bin is actually done via a move

  □ Consider 'moves' to the Recycle Bin as deletes

☑ Existing file is read from

☑ Existing file is written to

  ☑ Ignore file appends (this is useful for monitoring log file integrity)

150 Minimum # of bytes read or written in order to get reported

□ File is moved

□ File is renamed

□ File owner changed

□ File access permissions changed

□ File audit settings changed

For all checked actions, watch:

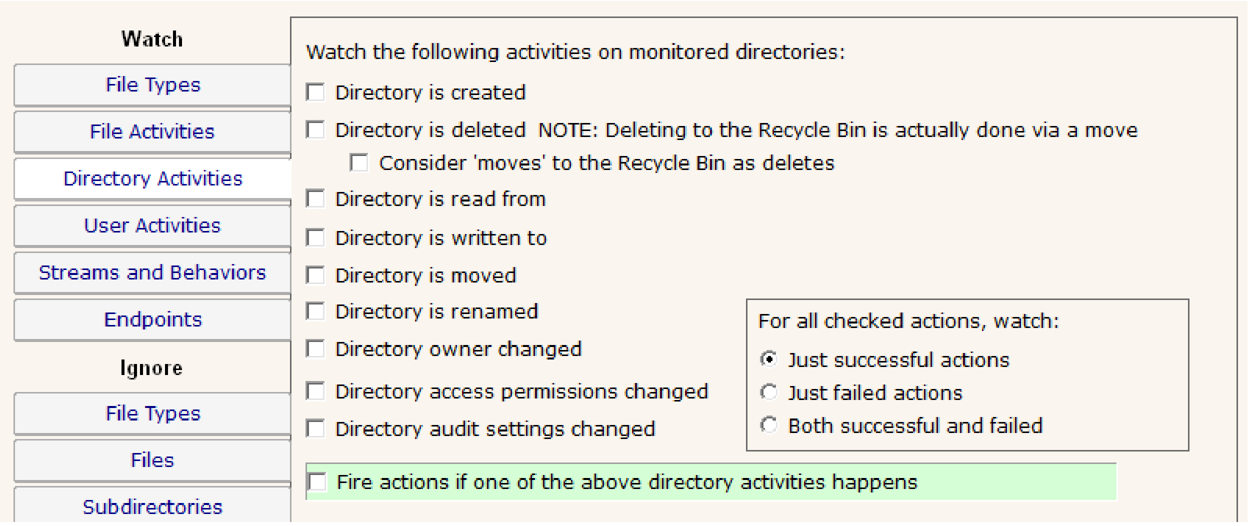
● Just successful actions

○ Just failed actions

○ Both successful and failed

□ Fire actions if the above file activities occur

Uncheck all of the boxes on the Directory Activities tab:



Watch the following activities on monitored directories:

☐ Directory is created

☐ Directory is deleted NOTE: Deleting to the Recycle Bin is actually done via a move

  ☐ Consider 'moves' to the Recycle Bin as deletes

☐ Directory is read from

☐ Directory is written to

☐ Directory is moved

☐ Directory is renamed

☐ Directory owner changed

☐ Directory access permissions changed

☐ Directory audit settings changed

For all checked actions, watch:

● Just successful actions

○ Just failed actions

○ Both successful and failed

☐ Fire actions if one of the above directory activities happens

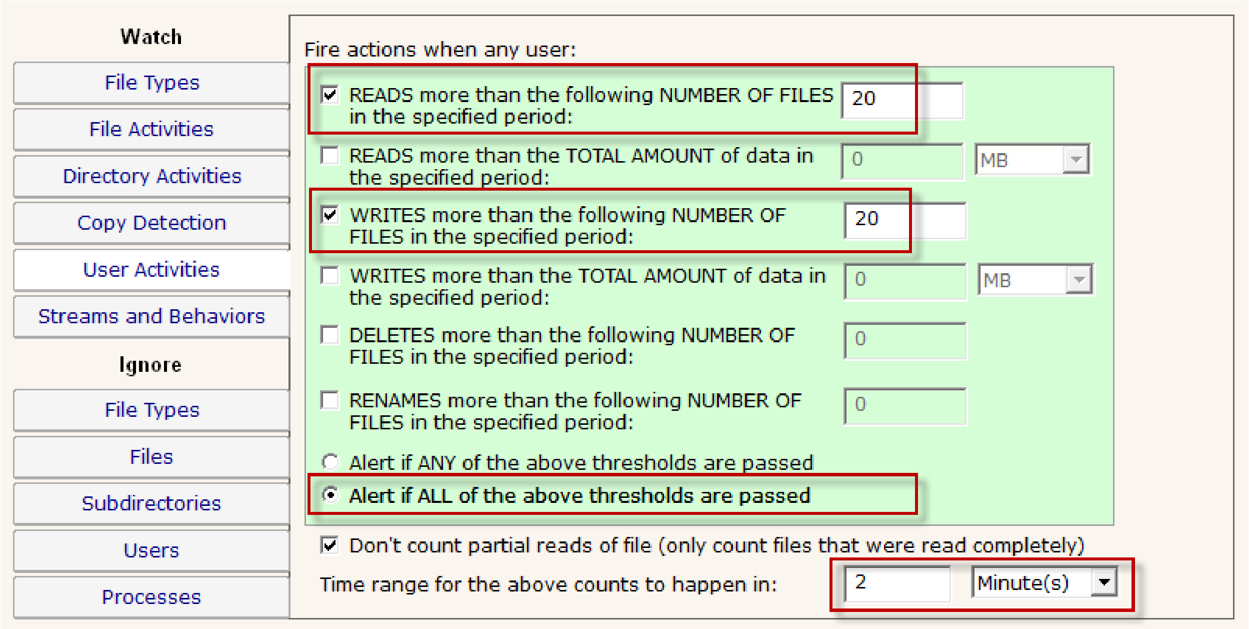
In order to be effective, ransomware has to encrypt files. That means it has to:

Read file contents from disk
Write encrypted file contents to disk

Some ransomware will write to a different file, and then delete the original file. Some will write into the original file, and possibly rename the file after it has been encrypted. Watching for deletes and renames would help cut down on false positives, but it will also miss any ransomware that doesn't do those final steps.

The User Activities tab is the most important. This is where the heuristic thresholds are defined. You want to set it such that a normal user is not impacted. Read AND writing 20 files in 2 minutes is unlikely for a normal user's workflow, and thus a safe threshold.

IMPORTANT: These threshold numbers are suggestions. The action is triggered as soon as the thresholds are passed, not at the end of the time period specified. Increasing the time gives more time for activity to accumulate towards the threshold. Therefore, increasing the time will increase the chance of catching a slow ransomware attack. But it also increases the chance of triggering on a normal user's work flow, so the threshold might need to be higher to prevent false positives.



Fire actions when any user:

☑ READS more than the following NUMBER OF FILES in the specified period: 20

☐ READS more than the TOTAL AMOUNT of data in the specified period: 0 MB

☑ WRITES more than the following NUMBER OF FILES in the specified period: 20

☐ WRITES more than the TOTAL AMOUNT of data in the specified period: 0 MB

☐ DELETES more than the following NUMBER OF FILES in the specified period: 0

☐ RENAMES more than the following NUMBER OF FILES in the specified period: 0

○ Alert if ANY of the above thresholds are passed

● Alert if ALL of the above thresholds are passed

☑ Don't count partial reads of file (only count files that were read completely)

Time range for the above counts to happen in: 2 Minute(s)

You can ignore the Streams and Behaviors and Endpoints tabs.

Ignores

For the Ignore tabs, it's best to ignore anything that might generate 'noise'. For example, a backup application will likely read all the files. There is no reason to record all of that information to the database, so it's best to ignore the backup process. Ignoring the anti-virus application is probably a good idea too. If you don't see those processes listed yet, give it some time and come back to the monitor. PA File Sight will add processes to the list as it sees them.

IMPORTANT: Do NOT ignore the System or Network process. When a user accesses files from across the network, the 'process' they are using will be reported as "System or Network".

If there are particular files you know are changed constantly (maybe things in a spool folder, a logs folder, etc), you could ignore that folder or those files.

Finally, consider if there are user accounts that should be ignored. Normal users should not normally be ignored, but rather any service accounts that might be used for specific operations. For example, if backups are performed by a specific backup account, that account could be ignored.

This monitor is now ready to start detecting ransomware attacks. After the other detection methods are discussed, we'll come back and look at adding actions to add prevention to the detection.

Detection via Honeypots

This method will work with all version of PA File Sight, not just the Ultra version.

The idea behind a honeypot is to create something tempting that only a ransomware application would touch, and something that humans should know not to touch. Typically this will be hidden folders with various files that would be tempting targets.

Often these folders are named something like **aaaHoneyPot** in hopes that the ransomware will scan that folder first (since it would sort to the top of a folder list). Unfortunately, there is no guarantee what order a ransomware will attack folders. In addition, at some point ransomware authors will get wiser and stop encrypting files in hidden folders. Even so, this is such a simple and inexpensive detection method it's worth setting up.

Create a few hidden folders inside your target folder. In this example we're protecting the D:\ folder, so create (for example):

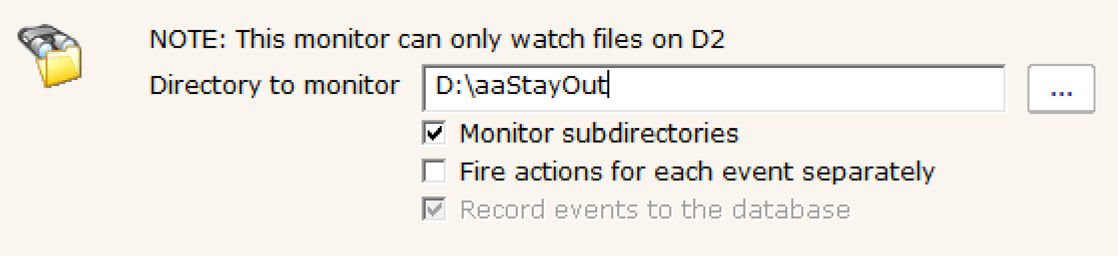
D:\aaStayOut

D:\zzStayOut

Make the folders hidden. Instruct your employees to never go into those folders.

Copy a few document files, spreadsheets, and PDFs into that folder. These should be files that are not critical, and could even be files you create now with non-important random data inside. Copy these files into both of the honeypot files mentioned above.

Now create two new File Sight monitors (one for each of the honey pot folders above).



NOTE: This monitor can only watch files on D2

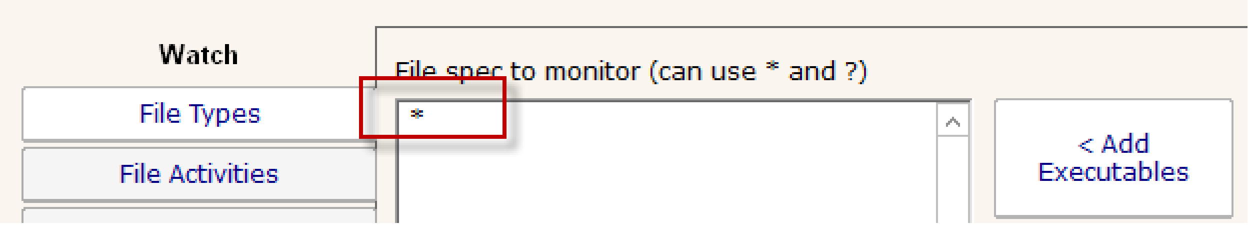
Directory to monitor D:\aaStayOut

☑ Monitor subdirectories

☐ Fire actions for each event separately

☑ Record events to the database

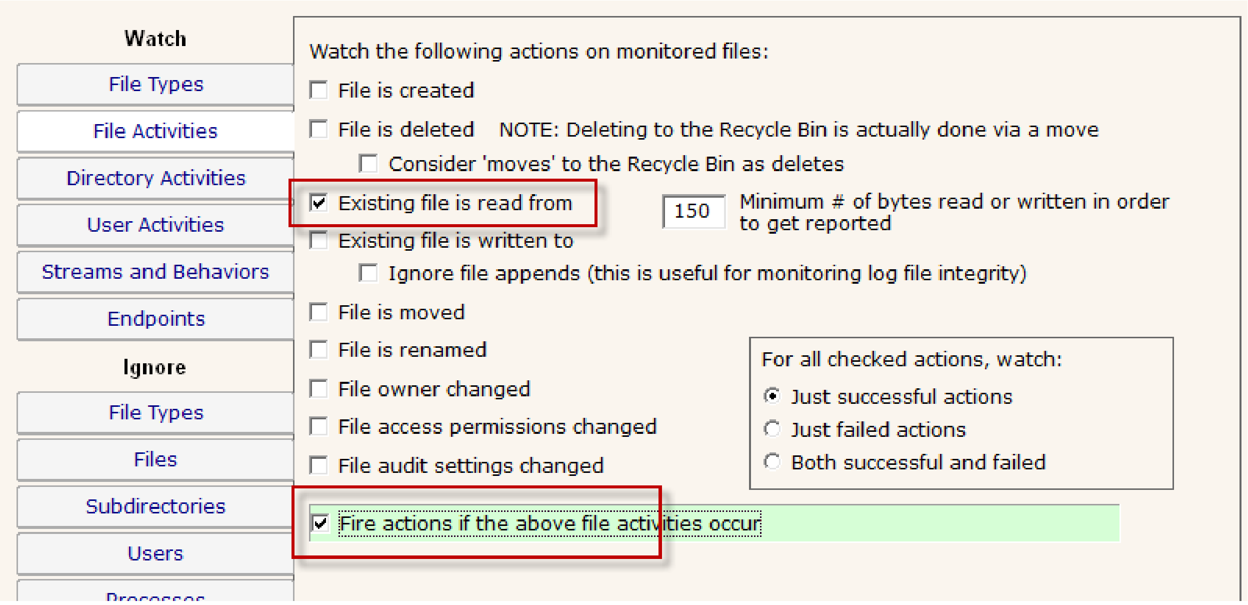
Watch all files on the File Types tab as shown below:



File spec to monitor (can use * and ?)

*

For the File Activities tab, we want to be notified (and run actions) if anyone reads any files in the honey pot folder:



Watch the following actions on monitored files:

☐ File is created

☐ File is deleted NOTE: Deleting to the Recycle Bin is actually done via a move

☐ Consider 'moves' to the Recycle Bin as deletes

☑ Existing file is read from

150 Minimum # of bytes read or written in order to get reported

☐ Existing file is written to

☐ Ignore file appends (this is useful for monitoring log file integrity)

☐ File is moved

☐ File is renamed

☐ File owner changed

☐ File access permissions changed

☐ File audit settings changed

For all checked actions, watch:

● Just successful actions

○ Just failed actions

○ Both successful and failed

☑ Fire actions if the above file activities occur

All the rest of the tabs can be left in their default state. Please look at the **Ignores** section above to ignore any users or processes that might end up reading all files (like a backup process) so they are not alerted on.

We're return to these monitors when we discuss Actions (prevention) below.

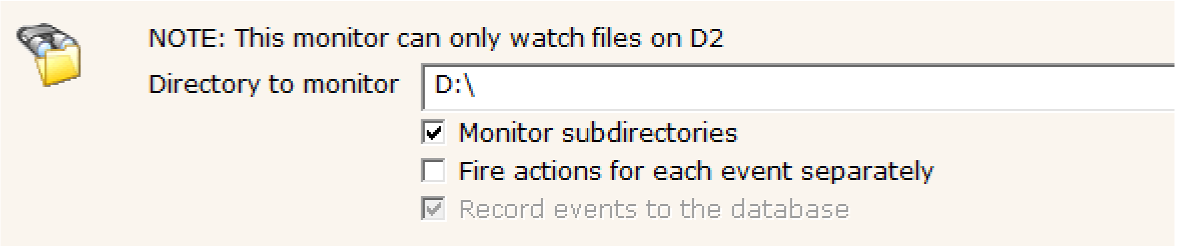
Detection via Encrypted File Extensions and Ransom Note Filenames

Most ransomware attacks will either leave a ransom note in the folders they attack, or they will rename the encrypted files with a new extension. For example, finance.xls might become finance.xls.encrypted after it has been encrypted.

There are a number of sites on the Internet that keep lists of file extensions and ransom note filenames that have been seen. PA File Sight can watch for these being written. The danger of course is any malware writer can change their malware to use different extensions and ransom note filenames.

Similar to the honey pots above though, this is a simple method that is simple to setup so it doesn't hurt to add it.

Create a new File Sight monitor to watch the target folder D:\



NOTE: This monitor can only watch files on D2

Directory to monitor: D:\

☑ Monitor subdirectories

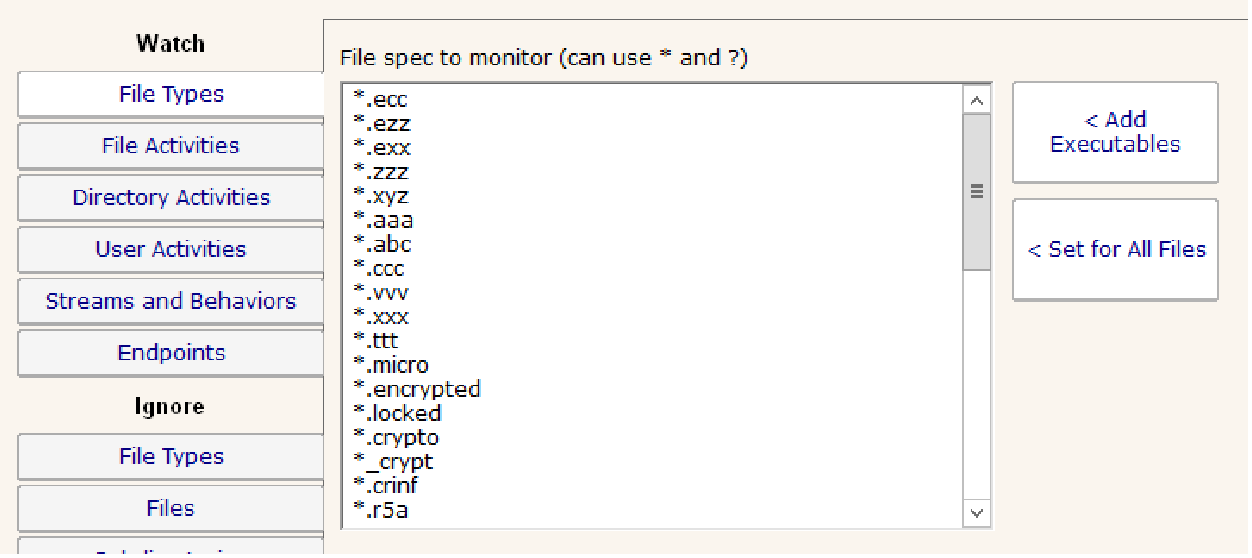
☐ Fire actions for each event separately

☑ Record events to the database

Get a list of typical encrypted file extensions. There is a list on the Power Admin Blog, with a reference to a page on Reddit.com that also has a list. These lists will always be outdated, but find the newest one you can to protect against the latest known ransomware variants.

On the File Types tab, you can replace the * and insert the list of file extensions you found. They need to be in the format of:

*.{extension} as shown in the screenshot below.



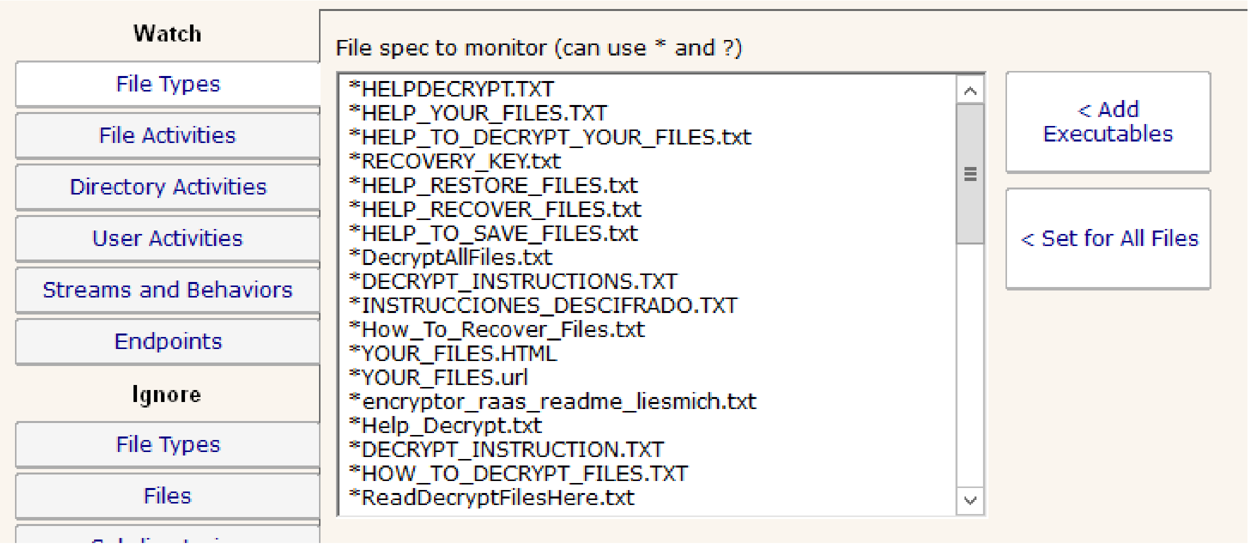
File spec to monitor (can use * and ?)

```
*.ecc
*.ezz
*.exx
*.zzz
*.xyz
*.aaa
*.abc
*.ccc
*.vvv
*.xxx
*.ttt
*.micro
*.encrypted
*.locked
*.crypto
*_crypt
*.crinf
*.r5a
```

Double check the list to make sure there aren't any file extensions that might be typically used at your location, and if there are, remove them.

You can also paste a list of ransom note filenames that are in the format of:

*{ransom note filename} as shown below:



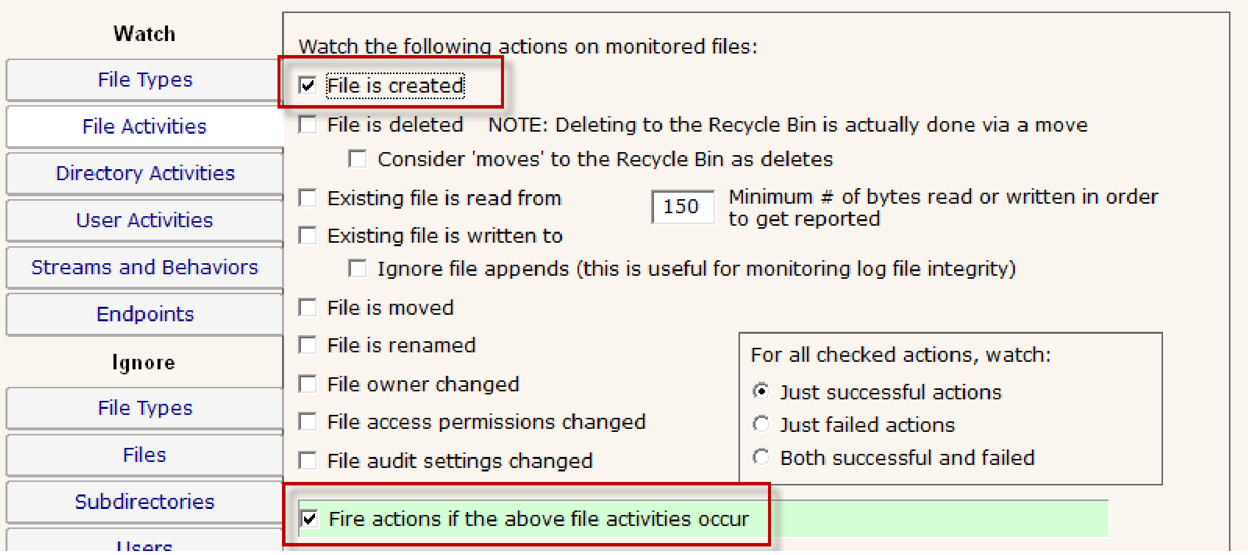
File spec to monitor (can use * and ?)

```
*HELPDECRYPT.TXT
*HELP_YOUR_FILES.TXT
*HELP_TO_DECRYPT_YOUR_FILES.txt
*RECOVERY_KEY.txt
*HELP_RESTORE_FILES.txt
*HELP_RECOVER_FILES.txt
*HELP_TO_SAVE_FILES.txt
*DecryptAllFiles.txt
*DECRYPT_INSTRUCTIONS.TXT
*INSTRUCCIONES_DESCIFRADO.TXT
*How_To_Recover_Files.txt
*YOUR_FILES.HTML
*YOUR_FILES.url
*encryptor_raas_readme_liesmich.txt
*Help_Decrypt.txt
*DECRYPT_INSTRUCTION.TXT
*HOW_TO_DECRYPT_FILES.TXT
*ReadDecryptFilesHere.txt
```

Be VERY careful and check this list of files carefully. Readme.txt is often included in these lists, but it is also a popular and legitimate filename.

Note that filenames and extensions are NOT case sensitive.

For the File Activities tab, we want to be alerted if a file is created that has one of the target extensions:



Watch the following actions on monitored files:

☑ File is created

☐ File is deleted   NOTE: Deleting to the Recycle Bin is actually done via a move

☐ Consider 'moves' to the Recycle Bin as deletes

☐ Existing file is read from   150   Minimum # of bytes read or written in order to get reported

☐ Existing file is written to

☐ Ignore file appends (this is useful for monitoring log file integrity)

☐ File is moved

☐ File is renamed

☐ File owner changed

☐ File access permissions changed

☐ File audit settings changed

For all checked actions, watch:

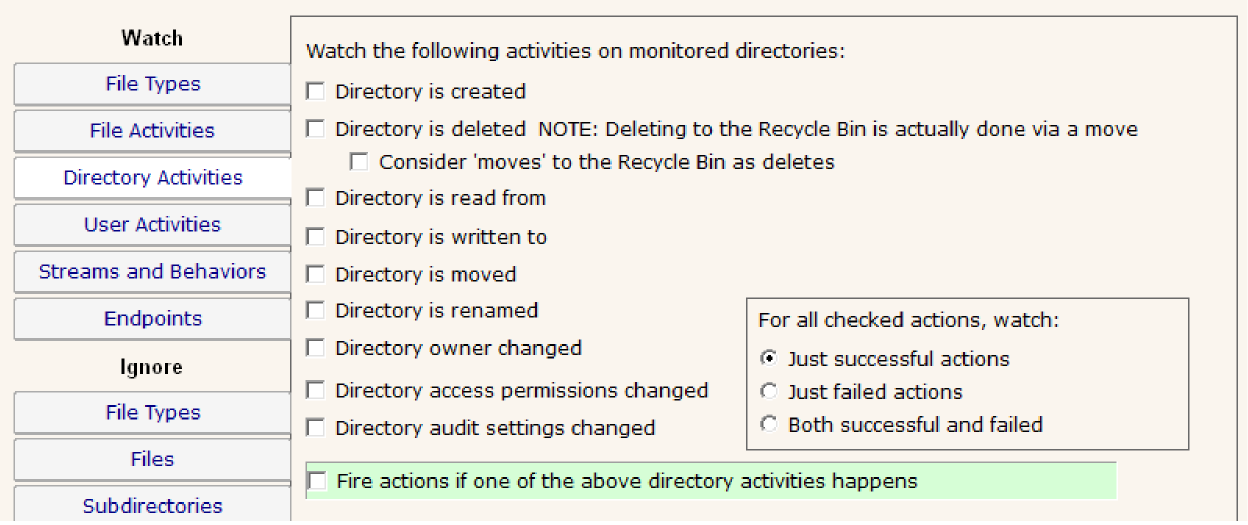
● Just successful actions

○ Just failed actions

○ Both successful and failed

☑ Fire actions if the above file activities occur

Uncheck everything on the Directory Activities tab:



Watch the following activities on monitored directories:

- □ Directory is created
- □ Directory is deleted NOTE: Deleting to the Recycle Bin is actually done via a move
  - □ Consider 'moves' to the Recycle Bin as deletes
- □ Directory is read from
- □ Directory is written to
- □ Directory is moved
- □ Directory is renamed
- □ Directory owner changed
- □ Directory access permissions changed
- □ Directory audit settings changed

For all checked actions, watch:

- ● Just successful actions
- ○ Just failed actions
- ○ Both successful and failed

□ Fire actions if one of the above directory activities happens

For this monitor, there isn't much reason to ignore anything. The rest of the tabs can be skipped.

Protection Responses

Once a ransomware attack has been detected using the monitors above, it needs to be stopped as soon as possible. This is done by adding one or more action to the monitors.

All of the monitors above should have an Email action attached which alerts IT staff to the problem so they can investigate.

Add to Blocked User List Action

An important additional approach is to automatically stop the compromised user account from harming any more files. This can be done with the **Add to Blocked User List** action. You can find more information here:

https://www.poweradmin.com/help/latestfshelp.aspx?page=action-add-to-blocked-users-list.aspx

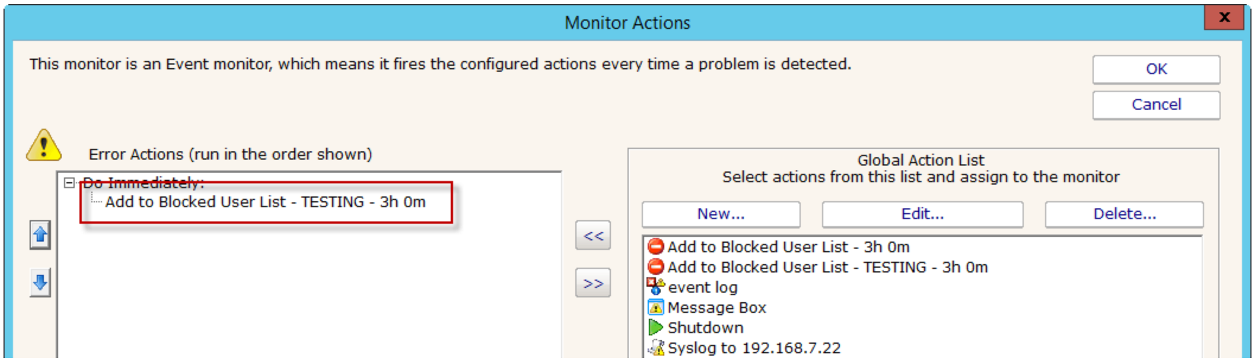
If you add this action to the above monitors, then as soon as the monitor fires actions, the user account that triggered the action will get added to the Blocked User List, and all attempts they make to create, read, write or delete files on the server will be blocked. The account will also get blocked on other drives that are monitored by PA File Sight within the same installation, including those monitored by Satellites.

IMPORTANT: The Blocked User List is a powerful tool. It can block a compromised account, but allow other normal users to continue working with the server without them knowing anything is wrong.

However, if an important user account, such as a service account used by a database for example, is blocked, it can cause problems for other software and other users. So it is important to do everything possible to reduce false positives.

One way you can reduce false positives is to test. There should be two Add to Blocked User List actions. One of them has the word “TESTING” added to the name. This action is completely safe – it will act just like the normal action, but it won’t actually block the triggered user account. With this in place, you can test your monitors for a few days to make sure nothing triggers them that shouldn’t. If you do get a false positive, you can probably fix it by changing an Ignore setting above.

So, go to all of the monitors you created above, and click the Actions button on each. Add the “Add to Blocked Users List – TESTING” action to the monitor.



Monitor Actions

This monitor is an Event monitor, which means it fires the configured actions every time a problem is detected.

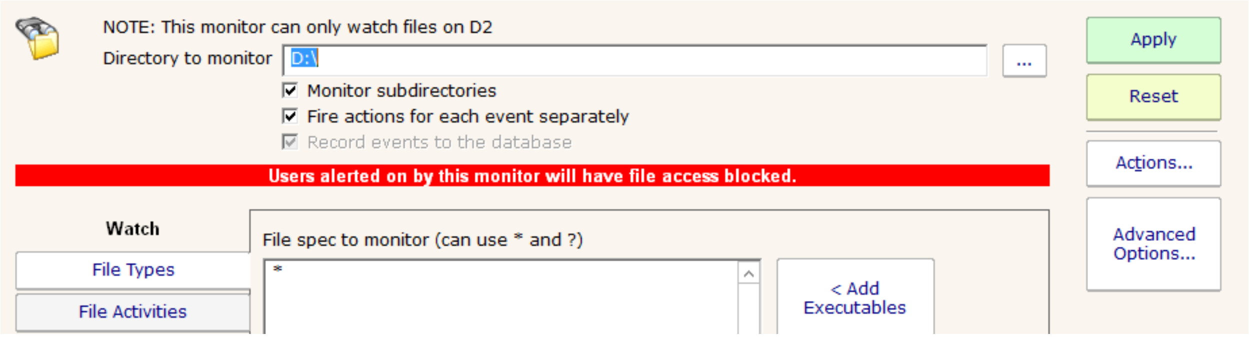
Error Actions (run in the order shown)

Do Immediately:
- Add to Blocked User List - TESTING - 3h 0m

Global Action List
Select actions from this list and assign to the monitor

- Add to Blocked User List - 3h 0m
- Add to Blocked User List - TESTING - 3h 0m
- event log
- Message Box
- Shutdown
- Syslog to 192.168.7.22

Once a PA File Sight monitor has a Add to Blocked User List action attached to it (even the TEST version), it will show a warning to remind you that this monitor can block user access.



NOTE: This monitor can only watch files on D2

Directory to monitor: D:\

☑ Monitor subdirectories
☑ Fire actions for each event separately
☑ Record events to the database

Users alerted on by this monitor will have file access blocked.

File spec to monitor (can use * and ?): *

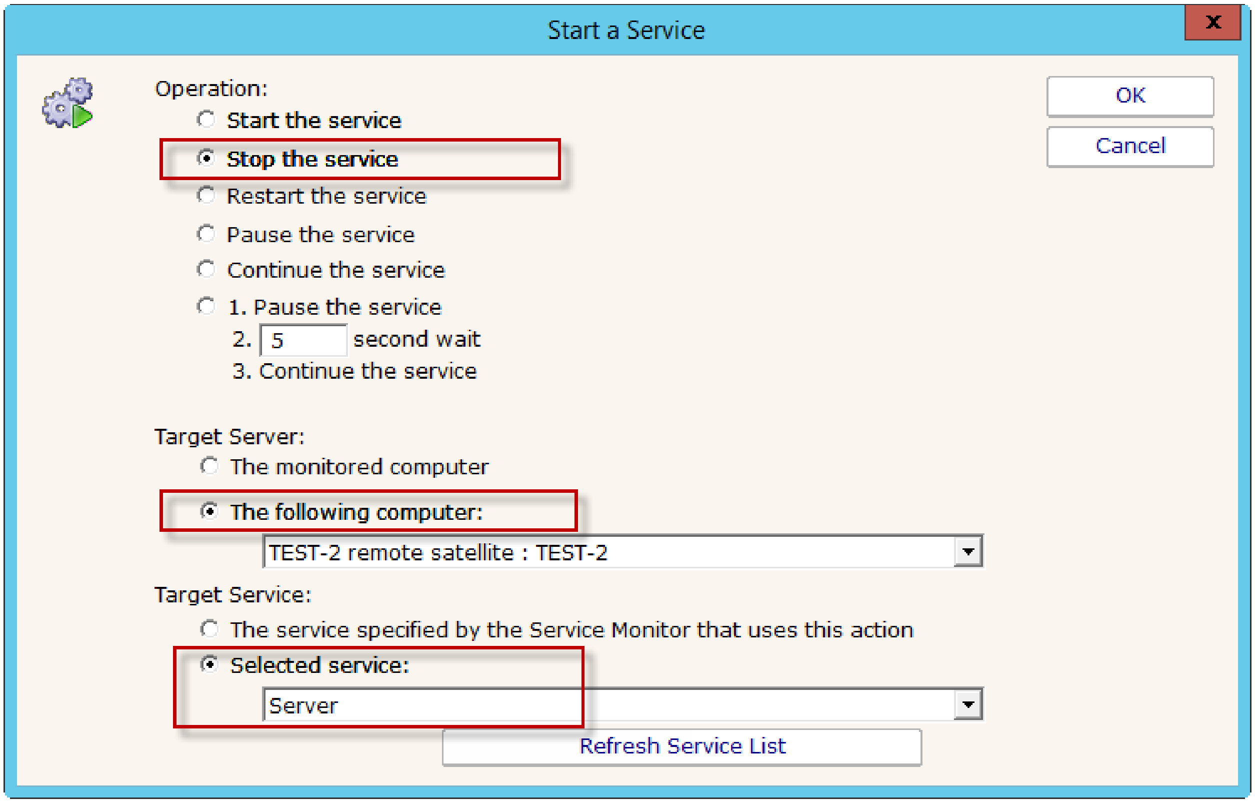
IMPORTANT: We highly recommend adding an Email action to any monitor that has an Add to Blocked User List action so IT is aware when any account is added to the list. The monitor will warn you if there isn’t an email action attached.

Stopping Services

An additional approach is to stop critical services on the server, such as the Server service (also called the Lanman Server service).

This service: "Supports file, print, and named-pipe sharing over the network for this computer. If this service is stopped, these functions will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start."

By stopping this service, ALL file access from the network to the server would be blocked. This can be done by adding the Start, Stop or Restart Service action as shown below:



Operation:

○ Start the service
● Stop the service
○ Restart the service
○ Pause the service
○ Continue the service
○ 1. Pause the service
2. 5 second wait
3. Continue the service

Target Server:

○ The monitored computer
● The following computer:
TEST-2 remote satellite : TEST-2

Target Service:

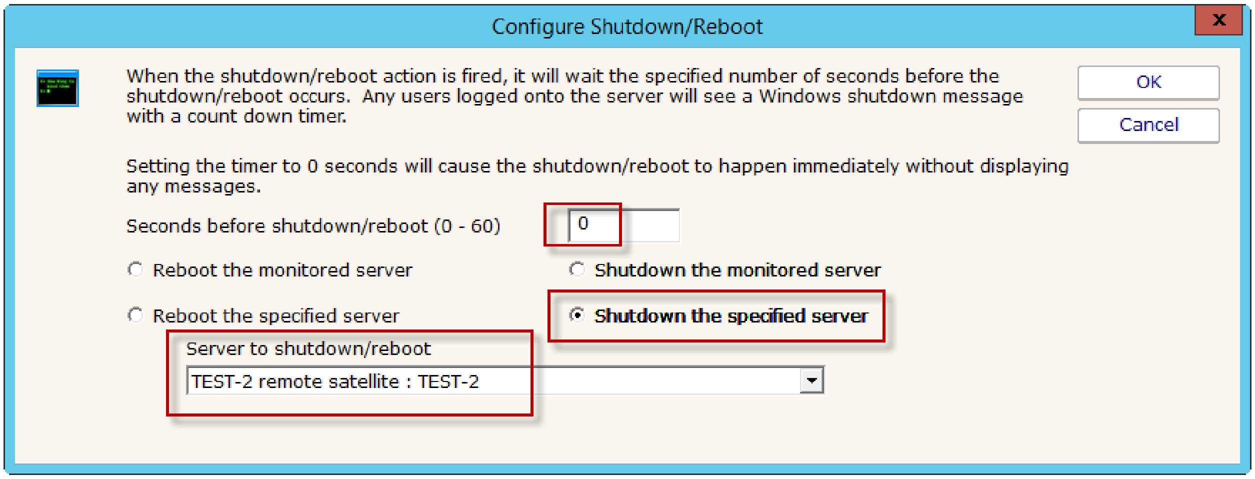
○ The service specified by the Service Monitor that uses this action
● Selected service:
Server

Note that you should specify the Target Server to be sure the service is stopped on the correct server when a Satellite Monitoring Service is in use.

Shutdown the Server

The safest, but possibly most disruptive protection mechanism would be to stop the server so nothing can be accessed.

In the example below, we've specified a zero second delay in shutting down the server – no reason to give the ransomware any extra time to cause trouble. Also note that this action would shutdown a specific server, which is important when using Satellites.



When the shutdown/reboot action is fired, it will wait the specified number of seconds before the shutdown/reboot occurs. Any users logged onto the server will see a Windows shutdown message with a count down timer.

Setting the timer to 0 seconds will cause the shutdown/reboot to happen immediately without displaying any messages.

Seconds before shutdown/reboot (0 - 60) 0

○ Reboot the monitored server ○ Shutdown the monitored server

○ Reboot the specified server ● Shutdown the specified server

Server to shutdown/reboot

TEST-2 remote satellite : TEST-2