

Forum:[Hack Forums](#)

Thread: [C# Grab names of files created and modified by specific process](#)

-PUBG- - February 19, 2019, 4:04 am

Title really says it all. I am trying to figure out a way to list all the files the have been modified or created even deleted through a specific process. I am attempting to accomplish this via C# any help is greatly appreciated.

Abruptum - February 19, 2019, 10:29 am

(Feb 19, 2019 05:04 AM)RapidHost™ Wrote: [\[CITE\]](#) Title really says it all. I am trying to figure out a way to list all the files the have been modified or created even deleted through a specific process. I am attempting to accomplish this via C# any help is greatly appreciated.

I would suggest this:

<https://stackoverflow.com/questions/4350717/how-can-i-detect-changes-to-files-from-windows>

0xDEAD10CC - February 19, 2019, 2:39 pm

(Feb 19, 2019 11:29 AM)Abruptum Wrote: [\[CITE\]](#) I would suggest this:

<https://stackoverflow.com/questions/4350717/how-can-i-detect-changes-to-files-from-windows>

Not even close to the right answer. This doesn't detect what process created/modified the file and it is also directory specific... You'd have to hook file writing methods within the target process, and that is the only real answer here.

Abruptum - February 20, 2019, 9:34 am

(Feb 19, 2019 03:39 PM)0xDEAD10CC Wrote: [\[CITE\]](#) Not even close to the right answer. This doesn't detect what process created/modified the file and it is also directory specific... You'd have to hook file writing methods within the target process, and that is the only real answer here.

Yes, you are right o.O seems like i totally misunderstood the question :/

Can you provide any source for your method ? i want to know how it can be done.

If proper created can it detect files changes runned through process chains ?

Really interesting topic.

0xDEAD10CC - February 20, 2019, 10:43 am

(Feb 20, 2019 10:34 AM)Abruptum Wrote: [\[CITE\]](#) Yes, you are right o.O seems like i totally misunderstood the question :/

Can you provide any source for your method ? i want to know how it can be done.

If proper created can it detect files changes runned through process chains ?

Really interesting topic.

Your hooks on functions like NtCreateFile, etc would indicate the changes, and would be applicable to the process you've created the hooks for.