Participation Activity 03 Assignment

NTFS Alternate Data Streams

Alternative Data Stream support was added to NTFS to help support Macintosh Hierarchical File System (HFS) that uses resource forks to store icons and other information for a file. While this is the intended use (as well as a few Windows internal functions), there are other uses for Alternative Data Streams that should concern system administrators and security professionals. Using Alternative Data Streams, a user can easily hide files that can go undetected unless closely inspected. In this assignment, you will learn how to manipulate and detect Alternative Data Streams. Alternative Data Streams is only supported on NTFS, not FAT file systems.

1. First, let’s get some practice creating your own Alternate Data Stream (AltDS). Bring up the **Command Prompt** application. With the following commands, we will create a new base file to hide behind:

**echo Nothing much going on in this file.>sample.txt**

**type sample.txt**

At this point, you should see the text "Nothing much going on in this file." that you redirected into the file **sample.txt**. Now, let’s display some of the file properties:

**dir sample.txt**

1. What is the size of the file in bytes? \_\_\_\_\_\_\_
2. Next, use the colon as the operator to tell our commands to create or use an AltDS:

**echo Pretty sneaky!>sample.txt:secret.txt**

Unfortunately, the use of the colon operator is a bit hit or miss in its implementation and sometimes does not work as we might expect:

**type sample.txt:secret.txt**

We should see some kind of error message displayed as the **type** command may not understand the colon operator, but we can use **notepad** to read the file and its AltDS.

1. Use the following command to bring up the file using **notepad**:

**notepad sample.txt**

Here, we should see the original "Nothing much going on in this file." in this file through **notepad**. Close **notepad** and then we’ll try to bring up the AltDS for this file.

**notepad sample.txt:secret.txt**

Hopefully, you see a **notepad** window with the text "Pretty sneaky!" in it.

1. Let’s take a look at the file properties again:

**dir sample.txt**

Notice that while the amount of total hard drive space free (may have) went down, the file size of **sample.txt** did not increase!

1. Open **Disk Investigator** and click **Yes** in the User Account Control dialog box. Under View with Disk selected, ensure that the **c: []** drive is selected in **Drive to view:** option.
2. What is the file system in use for this drive? \_\_\_\_\_\_\_
3. How many bytes are there per sector? \_\_\_\_\_\_\_
4. What is the cluster size? \_\_\_\_\_\_\_
5. Click the **Search** button, enter the complete text from above (i.e., **Nothing much going on in this file.**) in this file in the **Search for:** text field, make sure **Match case** is selected, and click **Search**. Since it may take several minutes, as soon as the tool indicates that it has found 1 matching result, you may stop the search. Click the **Locate Item** button to reveal the **Raw file contents** dialog box containing data from the file. You should have the **Text** and **Compact view** options checked in the **Raw file data**. Verify that you are able to see the hidden text and its AltDS file name as instructed above.
6. Go ahead and quit the Disk Investigator application.
7. Some anti-malware tools understand how to search Alternate Data Streams for malware. LADS by Frank Heyne is one freeware tool that seemed to work well for finding streams like the one we have just seen, but this information has now been incorporated into the **dir** command. Type **help dir** to see what option can help uncover any additional Alternate Data Streams.
8. What **dir** command option displays the alternate data streams of files? \_\_\_\_\_\_\_
9. What is the size of the AltDS hidden text in bytes? \_\_\_\_\_\_\_

You are to submit this document with your answers to the **Participation Activity 3** dropbox on Canvas by the due date and time. **No late submissions will be accepted.**