1.) Read and write will change the original file. We only care if it exist

if you read and write at the same time you can overtire the original file when you write to it so it will be blank, thus you need to make a copy first.

2.) cmd (write access only), notepad(read and write access) We use the dbg print and overwrote files and saw the ULONG for the access

3.) NtCreate file is used by notepad and cmd when creating a file that didn’t exist. NtOpen file is used when opening a file with read access by cmd or notepad. It also had access to the rename function.

4.) We know from our dbgprint that these functions are both called repeatedly upon booting the system. It is safe to assume the system uses these functions for booting, loading system tools and more.

NtOpen file is also used to access other objects such as volumes or directories, named pipes, mail slots

Gpc, Tcp Ucp Tcp6 network protocol so hardware devices like network cards are accessed through NtOpen

Net Bios, windows networking, WMIDataDevice

5.) This is likely to make the code easier, if they already a function capable of accessing many resources, why write a separate function for all resource types. This also allows the kernel to be smaller in size which is a good design choice for Microsoft to have a lighter kernel.

6.) The general purpose of NtSetInfrmationFile changes the provided information, changed information is determined by the FileInformationClasss, new information is taken form FileInformation buffer. If the file exists, then the caller must have specified that the target is to be replaced, otherwise an error is returned. We can use this to determine if the file exist. We can also use this to rename the file.

It also Sets the directory, Extended Attributes of the file, ObjectId information, Also for setting information for pipes, streams, and mail slots.

7.)

NtClose calls ObpCloseHandle obclose.c line 420

NtOpen Calls ObOpenObjectByName iosubs.c line 5588

NtSetFileInfomration Calls ObReferanceObjectByHandle qsinfo.c line 1561

8.) One gotcha that we addressed was the null pointer, we check to ensure that ObjectName is not null before intercepting the request to NtCreateFile

### notes for us from this mission ###

1048704 sometimes when txt opened

Notpad/cmd open file this happensULONG for read access 2148532352

Notepad ULONG for write access save file this happens 3222274176

Cmd dir > filename.txt ULONG 1074790528 so write acess?

Made when copy file ULONG 1074856064

Line 1195 qsifo.c create irp

Line 118 qsinfo.c NtSetInformationFile

Line 1451 gsinfo.c status

Line 2460 ntioapi.c copy file