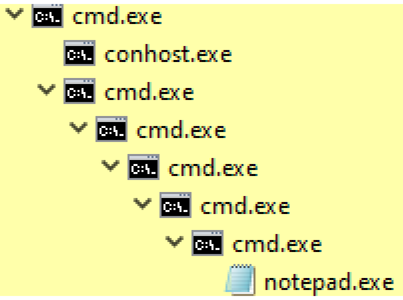
Trolololololobin and other lololololocoasters

hexacorn.com/blog/2021/10/09/trolololololobin-and-other-lololololocoasters

October 9, 2021 *in Living off the land, LOLBins*

In my older tweet I gave an example of a surgical way to inject process into a chain of executed programs and launch them at a predetermined position in a great-great-great….grand-parent-child relationship by using the *start* command:

```
start /b "" start /b "" start /b "" start /b "" start /b "" start /b notepad.exe
```



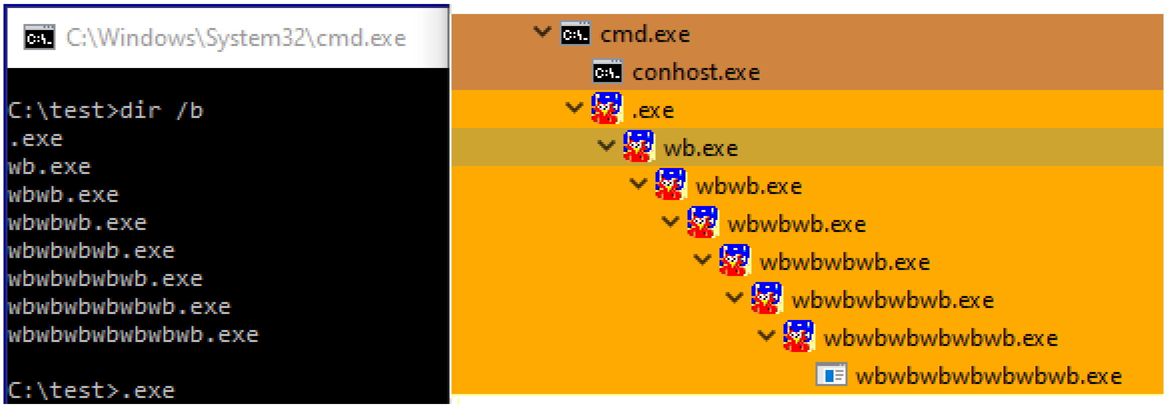
```
cmd.exe
    conhost.exe
    cmd.exe
        cmd.exe
            cmd.exe
                cmd.exe
                    cmd.exe
                        notepad.exe
```

Many Lolbins focus on loading DLLs, downloading files, etc. I was wondering if there is a class of Lolbins that could be used to generate this kinda process tree. The idea being that if we can find it, we can create more 'signed executable' chains and potentially disrupt parent-child relationship-based EDR detections.

After combing through my file collection I found one candidate and I suspect there will be others.

The Toshiba's signed *tinstall.exe* is an executable that is a part of many installs from this company. When launched, it spawns a child process which is a next step of the installation. The peculiar way it is doing it is providing us the feature I described above. When launched, it takes its own file name, and appends 'wb' to it, and then launches a program with that newly created name. Under normal circumstances, the name of the spawned process will be *tinstallwb.exe*.

By placing a number of copies of *tinstall.exe* in files named *.exe*, *wb.exe*, *wbwb.exe*, *wbwbwb.exe*, etc. we can build a chain of process spawned from signed executables with the *wbwbwbwbwbwbwb.exe* being the final 'payload':



```
C:\test>dir /b
.exe
wb.exe
wbwb.exe
wbwbwb.exe
wbwbwbwb.exe
wbwbwbwbwb.exe
wbwbwbwbwbwb.exe
wbwbwbwbwbwbwb.exe

C:\test>.exe
```

```
cmd.exe
    conhost.exe
    .exe
        wb.exe
            wbwb.exe
                wbwbwb.exe
                    wbwbwbwb.exe
                        wbwbwbwbwb.exe
                            wbwbwbwbwbwb.exe
                                wbwbwbwbwbwbwb.exe
```

Comments are closed.