Home Services Products & Freebies
Case Studies Contact Us
Search

Posted on **2022-01-16**

← Previous Next →

Beyond good ol' Run key, Part 135

These days I post most of the new stuff on Twitter as no one reads blogs anymore, right? 🙂

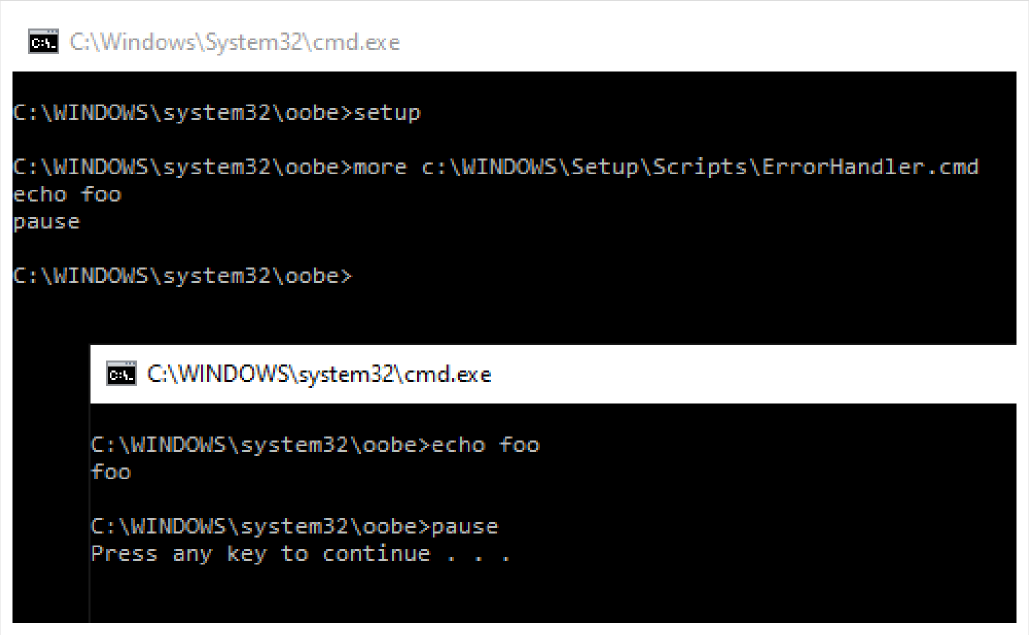
Still, good to document some of it in a more permanent way so this is the persistence bit I posted about yesterday:

A number of tools inside the c:\WINDOWS\system32\oobe\ folder:

- audit.exe
- oobeldr.exe
- Setup.exe
- windeploy.exe
- winsetup.dll

include references to c:\WINDOWS\Setup\Scripts\ErrorHandler.cmd.

Turns out, if you drop your payload to c:\WINDOWS\Setup\Scripts\ErrorHandler.cmd the c:\WINDOWS\system32\oobe\Setup.exe will load it anytime there is an error. The most trivial way to trigger it is by running setup.exe w/o any arguments.



```
C:\WINDOWS\system32\oobe>setup

C:\WINDOWS\system32\oobe>more c:\WINDOWS\Setup\Scripts\ErrorHandler.cmd
echo foo
pause

C:\WINDOWS\system32\oobe>
```

```
C:\WINDOWS\system32\oobe>echo foo
foo

C:\WINDOWS\system32\oobe>pause
Press any key to continue . . .
```

I have not checked the other executables, but it's most likely the case as well.

This entry was posted in **Autostart (Persistence)** by **adam**. Bookmark the **permalink**.