

Beyond good ol' Run key, Part 137

 hexacorn.com/blog/2022/01/22/beyond-good-ol-run-key-part-137

January 22, 2022 in [Autostart \(Persistence\)](#)

This is a neat persistence trick you can use... if you got access to TrustedInstaller...

The *wininet.dll* library in Windows 10+ extends the functionality of *InternetErrorDlg* function to reach out to a configurable Registry location that supports handling of unknown error messages. The function takes the error code as an argument and reaches out to the following location:

```
HKLM\SOFTWARE\Microsoft\Windows\
CurrentVersion\Internet Settings\LUI\<error>
```

It then reads the value in a form of an expandable string and extracts library name from it by splitting it from the exported API name using an exclamation mark as a separator. And if a given error code doesn't have an entry the function defaults to value 'o' which by default points to:

```
%SystemRoot%\system32\wininetlui.dll!InternetErrorDlgEx
```

I was curious if I could force the loading of my own payload and after launching Process Monitor with a filter on \Lui path I was able to quickly trigger error 12040 (ERROR_INTERNET_HTTPS_TO_HTTP_ON_REDIRECT). I then added an entry for my own test library and was able to load my DLL

The screenshot displays a sequence of registry operations performed by Internet Explorer (IE) processes. The operations include opening, setting, querying, and closing registry keys, as well as creating and querying files. A DebugView window shows the following debug print output:

#	Time	Debug Print
1	0.00000000	[2704] DLLMain_32_DLL_PROCESS_ATTACH
2	0.00134840	[2704] DLLMain_32_DLL_PROCESS_DETACH
3	71.10634613	[2704] DLLMain_32_DLL_PROCESS_ATTACH
4	71.10788727	[2704] DLLMain_32_DLL_PROCESS_DETACH

The Registry Editor window shows the path `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\LUI`. The registry values are as follows:

Name	Type	Data
(Default)	REG_SZ	(value not set)
0	REG_EXPAND_SZ	%SystemRoot%\system32\wininet\ui.dll\InternetErrorDlgEx
12040	REG_SZ	c:\test\test32.dll\foobar

There are at least two caveats:

- You need TrustedInstaller rights to add/modify the registry entry
- User needs to use Internet Explorer (I couldn't trigger it in Edge)

Comments are closed.