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…

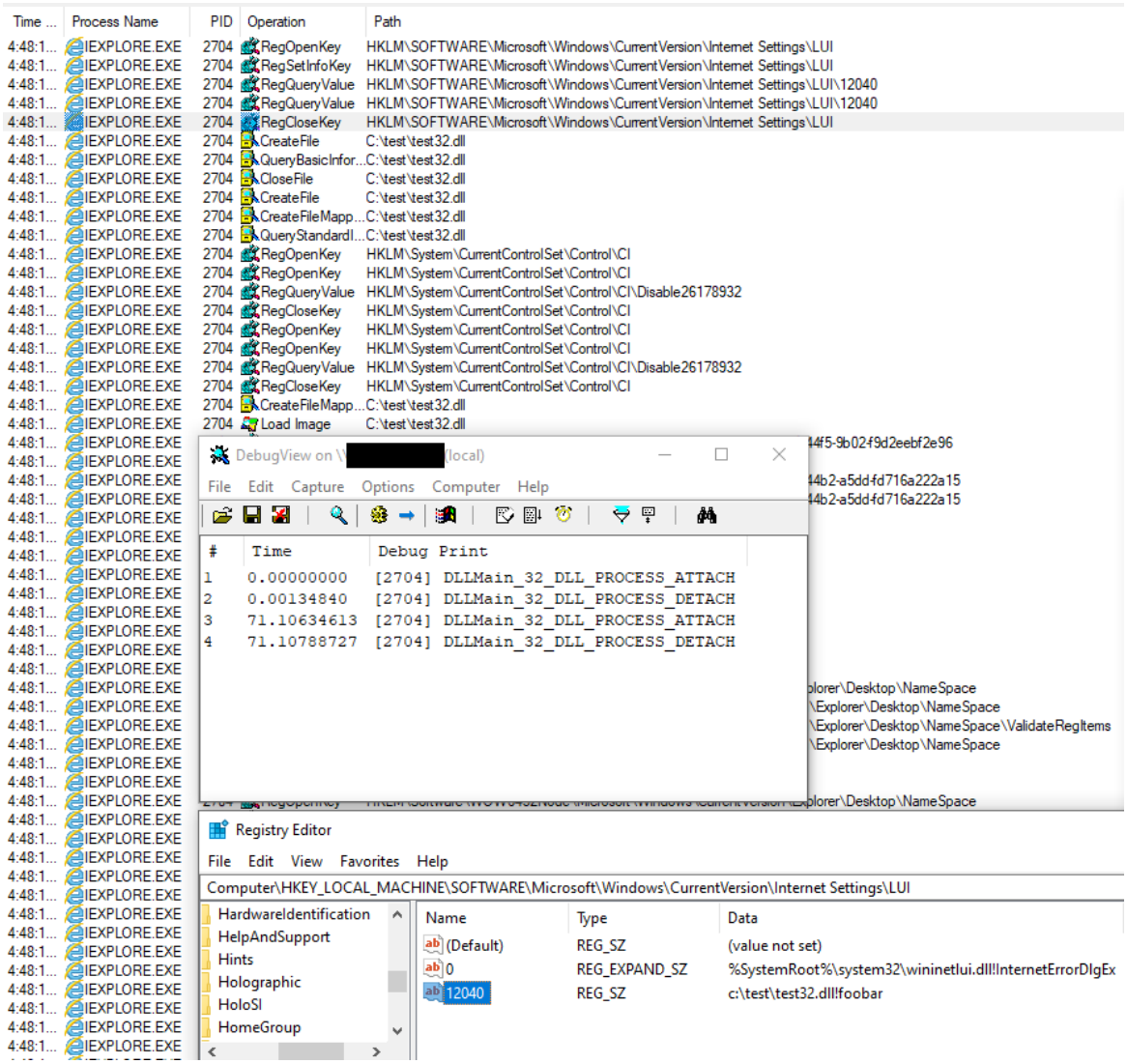
The *wininet.dll* library in Windows 10+ extends the functionality of *InternetErrorDlg* function to reach out to a configurable Registry location that supports handling of unknown error messages. The function takes the error code as an argument and reaches out to the following location:

```
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 '0' 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_REDIR). I then added an entry for my own test library and was able to load my DLL



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.