Beyond good ol' Run key, Part 131

February 6, 2021 *in Anti-Forensics, Autostart (Persistence)*

This is a bunch of legacy and not so popular anymore Registry locations that could have at some stage in the past support persistence by pointing to various editors associated with 'viewing source of web pages', and using Microsoft Office for editing HTML documents:

- HKCU\Software\Microsoft\Shared\HTML\Default Editor
- HKCU\SOFTWARE\Microsoft\Shared\HTML\Old Default Editor
- HKLM\SOFTWARE\Microsoft\Shared\HTML\Old Default Editor
- HKCU\Software\Microsoft\Internet Explorer\Default HTML Editor
- HKCU\Software\Microsoft\Internet Explorer\Default MHTML Editor
- HKLM\Software\Microsoft\Internet Explorer\Default HTML Editor
- HKLM\Software\Microsoft\Internet Explorer\Default MHTML Editor
- HKLM\Software\Wow6432Node\Microsoft\Internet Explorer\Default HTML Editor
- HKLM\Software\Wow6432Node\Microsoft\Internet Explorer\Default MHTML Editor

All the entries use the very same shell entries as shown on the below example: