Beyond good ol' Run key, Part 98

Scanning the Windows files for possible persistence mechanisms I came across a few interesting strings inside the Natural Language Development Platform 6 library (NaturalLanguage6.dll):

- StemmerDLLPathOverride
- WBDLLPathOverride
- StemmerClass
- WBreakerClass

Quick google exercise followed and I found this post in Russian that explains that these are actual Registry entries – by changing them the author was able to use Russian morphology modules for searches on Sharepoint.

Cool.

Now that I had an idea what it is, I was curious if the entries are used on Windows 10.

Procmon with boot logging enabled confirmed that it is the case – the C:\WINDOWS\system32\SearchIndexer.exe process looks for the DLLOverridePath entries under the following locations (language may vary on non-English OS versions):

- HKLM\System\CurrentControlSet\Control\ContentIndex\Language\English_UK
- HKLM\System\CurrentControlSet\Control\ContentIndex\Language\English_US
- HKLM\System\CurrentControlSet\Control\ContentIndex\Language\Neutral

Time of Day	Process Name	PID	Operation	Path	Result
5:08:10.7959521 PM	SearchIndexer....	2548	RegQueryVa...	HKLM\System\CurrentControlSet\Control\ContentIndex\Language\English_UK\WBDLLPathOverride	NAME NOT FOUND
5:08:10.7962435 PM	SearchIndexer....	2548	RegQueryVa...	HKLM\System\CurrentControlSet\Control\ContentIndex\Language\English_US\WBDLLPathOverride	NAME NOT FOUND
5:08:10.8004604 PM	SearchIndexer....	2548	RegQueryVa...	HKLM\System\CurrentControlSet\Control\ContentIndex\Language\English_UK\StemmerDLLPathOverride	NAME NOT FOUND
5:08:10.8005824 PM	SearchIndexer....	2548	RegQueryVa...	HKLM\System\CurrentControlSet\Control\ContentIndex\Language\English_US\StemmerDLLPathOverride	NAME NOT FOUND
5:08:10.8843865 PM	SearchIndexer....	2548	RegQueryVa...	HKLM\System\CurrentControlSet\Control\ContentIndex\Language\Neutral\WBDLLPathOverride	NAME NOT FOUND

Since the overridden locations are loaded via LoadLibrary, it is yet another persistence location to look at.

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