Beyond good ol' Run key, Part 78

Here's a quick persistence mechanism for you: we all know that you can change the HKCR settings for file extensions to introduce a malicious proxy executable that can then launch the appropriate file. Changes to HKCR's .exe, .txt, handlers are as old as Windows malware itself.

It turns out that you can apply the same trick to folders, and you can do so with an extra twist. To do so, just add these Registry entries:

- HKCR\Folder\shell\(default)=test
- HKCR\Folder\shell\test\command @="notepad.exe"

And from now on, anytime you open any folder in Windows Explorer the notepad.exe will launch. And for the twist – note that we are introducing a new 'verb' called 'test' for Shell and not modifying the 'open' command; spotting this may be much harder as you need the security solution to read what the default verb is first, then read its settings from the Registry. You can leverage this trick to modify shell's behavior for any file type.

Obviously, such changes may ruin the user's folder browsing experience, but Notepad is now a folder parasite and is here to stay…

If you wanted to be a bit more sneaky, and apply it to specific folders only, e.g. Recycle Bin, you just need to add (in this case we modify the 'open' verb settings, for simplicity):

HKCR\CLSID\{645FF040-5081-101B-9F08-00AA002F954E}\shell\open\command @="c:\\windows\\system32\\calc.exe"

Where the 645FF040-5081-101B-9F08-00AA002F954E CLSID refers to Recycle Bin folder. Same goes for other special folders (as long as they are supported on your Windows version – win8/10 changes a lot here as they introduce that awful AOLish Start Menu).

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