**13Cubed- ShellBag Forensics**

**High level overview of shellbags**

Shellbag Locations (Windows Vista and Later)-

NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU

NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags

UsrClass.dat\Local Settings\Software\Microsoft\Windows\Shell\BagMRU

UsrClass.dat\Local Settings\Software\Microsoft\Windows\Shell\Bags

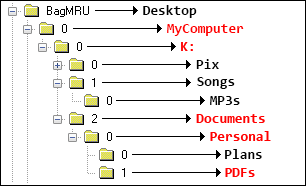
Ntuser 🡪 some data, Usrclass 🡪 most

Paths of both .dat files are mentioned initially.

Shellbags are created for zip files as well.

Even deleted files/ folders/ drives, etc. can be viewed in shellbags.

* BagMRU: Shows us the actual directory structures of which folders were interacted with in the format of numbered subkey/value hierarchies.
  + e.g. the Windows 7 registry path UsrClass.dat\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\0\0\2\0\1



Manual methods to access shellbags are referenced in “https://www.4n6k.com/2013/12/shellbags-forensics-addressing.html”

MRUListEx: Order in which folders were last accessed.

NodeSlot: Points to Bag key, which stores customization data.

NodeSlots: It is updated upon new shellbags creation.

Bags: Contains numbered subkeys for each hierarchical child subkey under BagMRU

Windows Shellbag Parser, Shellbags.py, Shellbags explorer, internt evidence finder

Shellbags explorer 🡪

Cmd and GUI versions

Cmd – SBECmd.exe -l –csv .\ 🡪 Exported file saved as .tsv (tab separated value) extension

.tsv headers 🡪 BagPath, MRUPositions, Absolute Path, ShellType, Value, No. of childbags, created on, modified on, accessed on, last write time, etc.

Gui – Shellbags explorer.

He opened shellbags information for live registry.