

Mason Competitive Cyber

Windows Registry Deep Dive



Recent Competitions



- VTSummit
- NCL

Upcoming Competitions & Events



- UMDCTF
 - In-person @UMD on Sat
- Online CTFs
 - Check #ctfwatch

El Plan

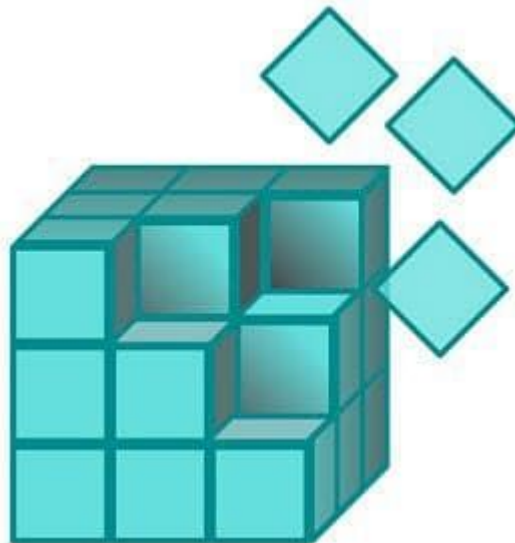


- What is the Registry?
- How is it structured?
- Forensic artifacts in the registry
- Hacking the registry 🤪

What is the Windows Registry

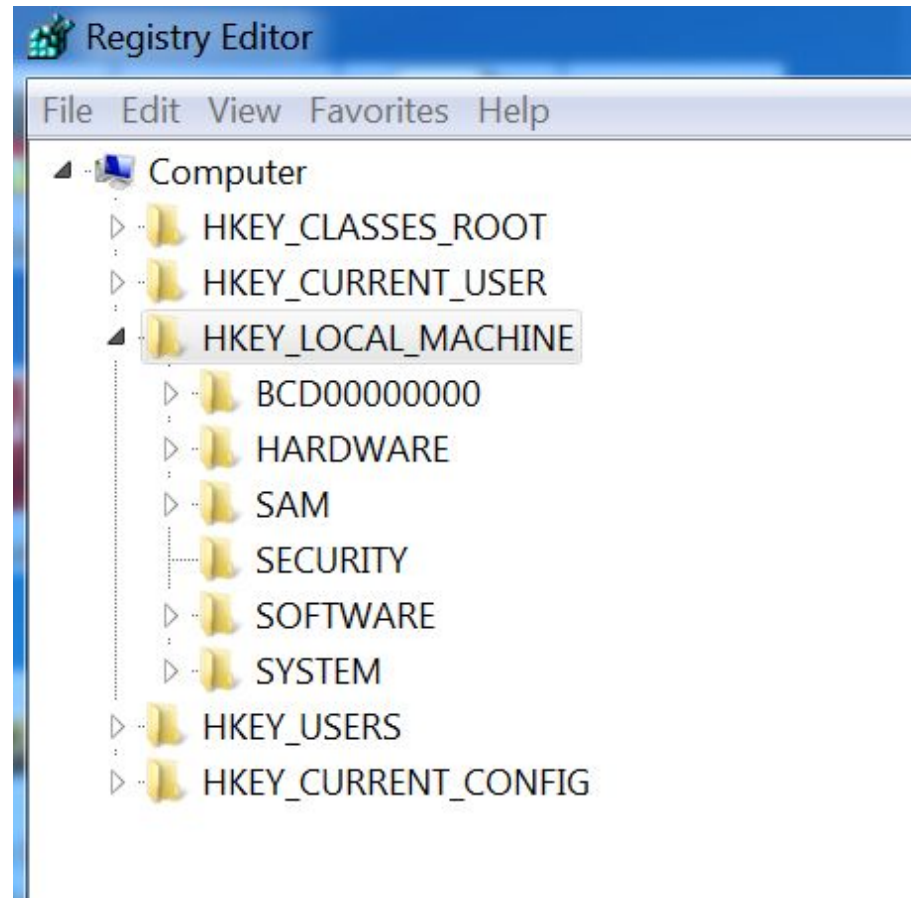


- If you know it's probably because you've had a serious error with your system
- **Windows Registry** - database that stores important settings about OS and installed programs
 - Replaced INI files
- Disclaimer: BE CAREFUL. The registry has no “Save” or “Undo”

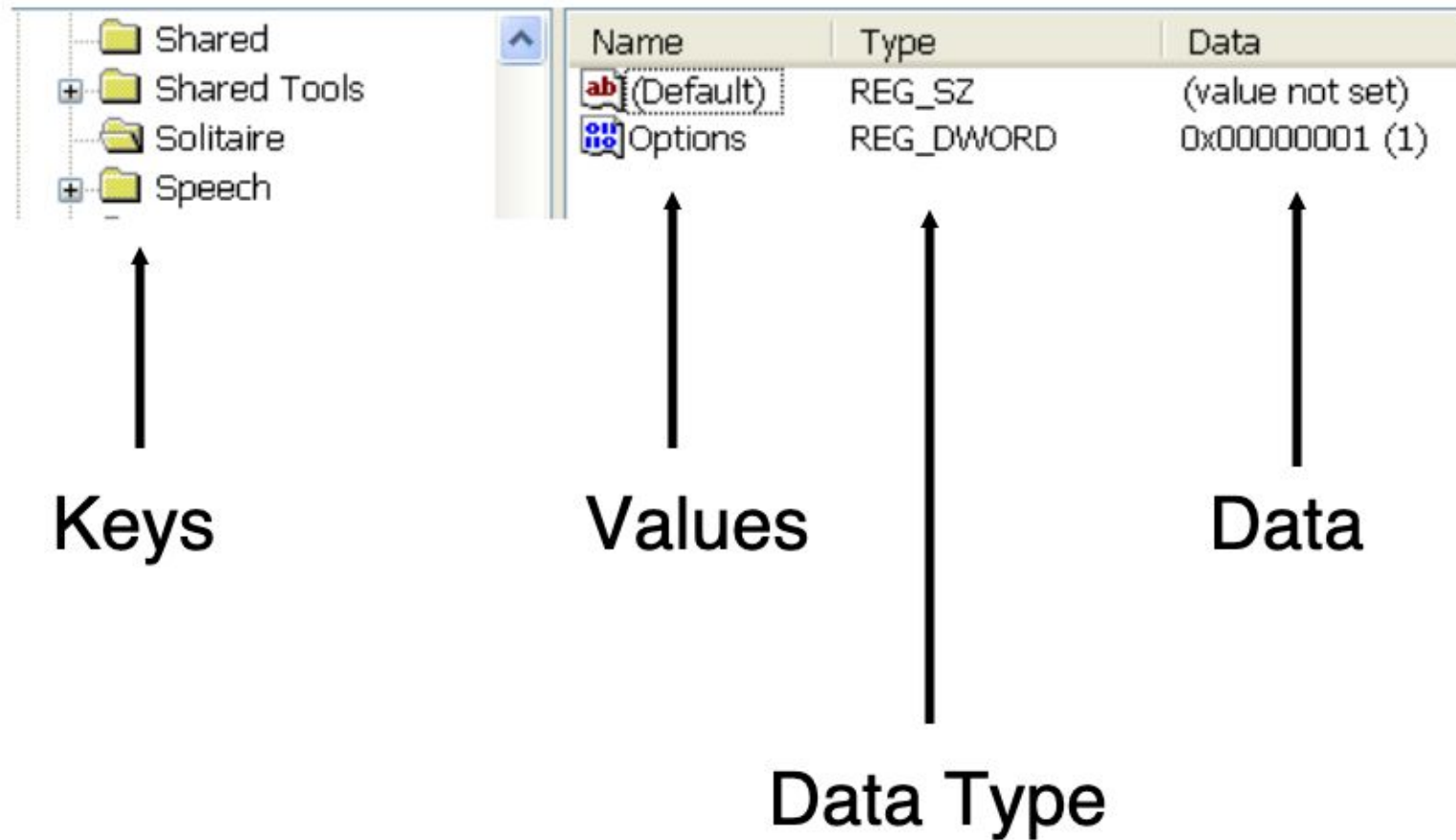


Registry Structure

- Binary hierarchical database
 - Based on nodes (keys, values) and pointers
- Hives → files
 - REGF binary format
- /system32/config
 - SYSTEM
 - SOFTWARE
 - SAM
 - Security
- User info
 - USRCLASS.DAT
 - NTUSER.DAT
- regedit.exe
 - GUI tool for registry



Registry Structure



The Registry as a log file

- Keys have a lastwritetime
 - 64bit filetime
 - for key itself NOT content
- Some keys have timestamps within their value's data
 - 64bit filetime OR 32bit FATtime
- Helps with timelining

UserAssist



Name	Type	Data
 P:\Hfref\Unpxre\Qrfxgbc\pelcfnehf-UhtuWnff.rkr	REG_BINARY	02 00 0
 P:\Hfref\Unpxre\Qrfxgbc\pelcfnehf-urnil.rkr	REG_BINARY	02 00 0
 P:\Hfref\Unpxre\Qrfxgbc\pelcfnehf-urnilurnilur...	REG_BINARY	02 00 0
 P:\Hfref\Unpxre\Qrfxgbc\pelcfnehf-urnilynfg.rkr	REG_BINARY	02 00 0
 P:\Hfref\Unpxre\Qrfxgbc\PelcfnehfUvqr.rkr	REG_BINARY	02 00 0
 P:\Hfref\Unpxre\Qrfxgbc\pelcfnehf-uvqrnaqfrx...	REG_BINARY	02 00 0
 P:\Hfref\Unpxre\Qrfxgbc\pelcfnehf-uzffsgc.rkr	REG_BINARY	02 00 0
 P:\Hfref\Unpxre\Qrfxgbc\pelcfnehf-uzfgnavhz.r...	REG_BINARY	02 00 0
 P:\Hfref\Unpxre\Qrfxgbc\pelcfnehf-uzfubfg2.rkr	REG_BINARY	02 00 0
 P:\Hfref\Unpxre\Qrfxgbc\pelcfnehf-vgjbexfybp...	REG_BINARY	02 00 0
 P:\Hfref\Unpxre\Qrfxgbc\pelcfnehf-vqrohtgure...	REG_BINARY	02 00 0
 P:\Hfref\Unpxre\Qrfxgbc\pelcfnehf-vs dhvmrfn...	REG_BINARY	02 00 0
 P:\Hfref\Unpxre\Qrfxgbc\pelcfnehf-vsguvfqbrf...	REG_BINARY	02 00 0
 P:\Hfref\Unpxre\Qrfxgbc\pelcfnehf-vsguvfqbrf...	REG_BINARY	02 00 0

UserAssist



- ROT13 lol
- Program Execution
- GUID
- Filepath
- Timestamp

Name	Type	Data
P:\Hfref\Unpxre\Qrfxgbc\pelcfnehf-UhtuWnff.rkr	REG_BINARY	02 00 0
P:\Hfref\Unpxre\Qrfxgbc\pelcfnehf-urnil.rkr	REG_BINARY	02 00 0
P:\Hfref\Unpxre\Qrfxgbc\pelcfnehf-urnilurnilur...	REG_BINARY	02 00 0
P:\Hfref\Unpxre\Qrfxgbc\pelcfnehf-urnilynfg.rkr	REG_BINARY	02 00 0
P:\Hfref\Unpxre\Qrfxgbc\pelcfnehf-Uvqr.rkr	REG_BINARY	02 00 0
P:\Hfref\Unpxre\Qrfxgbc\pelcfnehf-uvqrnaqfrx...	REG_BINARY	02 00 0
P:\Hfref\Unpxre\Qrfxgbc\pelcfnehf-uzffsgc.rkr	REG_BINARY	02 00 0
P:\Hfref\Unpxre\Qrfxgbc\pelcfnehf-uzfgnavhz.r...	REG_BINARY	02 00 0
P:\Hfref\Unpxre\Qrfxgbc\pelcfnehf-uzfubfg2.rkr	REG_BINARY	02 00 0
P:\Hfref\Unpxre\Qrfxgbc\pelcfnehf-vgjbexfybp...	REG_BINARY	02 00 0
P:\Hfref\Unpxre\Qrfxgbc\pelcfnehf-vqrohtgure...	REG_BINARY	02 00 0
P:\Hfref\Unpxre\Qrfxgbc\pelcfnehf-vs dhvmrfn...	REG_BINARY	02 00 0
P:\Hfref\Unpxre\Qrfxgbc\pelcfnehf-vsguvfqbfr...	REG_BINARY	02 00 0
P:\Hfref\Unpxre\Qrfxgbc\pelcfnehf-vsguvfqbfr...	REG_BINARY	02 00 0





What useful info is in the registry?



- Application settings
- Autorun information
 - Might not be in startup folder
- Formerly attached USB devices
- User activity
 - MRUs
 - Viewed documents
 - Applications installed or run

The Run Key

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
 - Commands to run each time a user LOGS IN
 - Not in order
 - Both for HKLM and HKCU
- Can add values to key
 - Need admin

	Adobe Reader Speed Launcher	REG_SZ	"C:\Program Files\Adobe\Reader 8.0\Reader\Reader_sl.exe"
	Broadcom Wireless Manager UI	REG_SZ	C:\WINDOWS\system32\WLTRAY.exe
	DLA	REG_SZ	C:\WINDOWS\System32\DLA\DLACTRLW.EXE
	DVDLauncher	REG_SZ	"C:\Program Files\CyberLink\PowerDVD\DVDLauncher.exe"

Command Processor/Autorun

- HKLM\SOFTWARE\Microsoft\Command Processor
 - Commands to run every time cmd.exe starts
 - For each user or for system

exefile\shell\open\command

- HKLM\Software\Classes\exefile\shell\open\command
 - Default entry should be “%1” %*
 - Run every time an exe file is open
 - Pretty Park malware
 - Old worm
 - Ran malware exe every time any exe run

SAM hive



- Local user account info
- Local group account info

User Information

```
-----
Username       : Administrator [500]
Full Name      :
User Comment    : Built-in account for administering the computer/domain
Account Type    : Default Admin User
Account Created : Tue Sep  3 08:48:07 2002 Z
Last Login Date : Fri Nov  9 17:12:55 2018 Z
Pwd Reset Date  : Fri Nov  9 16:49:58 2018 Z
Pwd Fail Date   : Tue Dec  1 11:55:08 2009 Z
Login Count     : 50
--> Normal user account
--> Password does not expire
```

- Stores audit policy
 - Like running auditpol.exe on live system
- What you expect to see in event logs

```
auditpol
Policy\PolAdtEv
LastWrite Time Fri Nov 9 18:06:59 2018 (UTC)

Length of data: 44 bytes.
0x00000000: 01 17 f5 77 03 00 00 00 03 00 00 00 02 00 00 00 ...w.....
0x00000010: 00 00 00 00 00 00 00 00 02 00 00 00 03 00 00 00 .....
0x00000020: 03 00 00 00 03 00 00 00 09 00 00 00 .....
Auditing is enabled.
    Audit System Events           = S/F
    Audit Logon Events            = S/F
    Audit Object Access           = F
    Audit Privilege Use           = N
    Audit Process Tracking        = N
    Audit Policy Change           = F
    Audit Account Management      = S/F
    Audit Dir Service Access      = S/F
    Audit Account Logon Events    = S/F
-----
```


AppCompat



- Shimcache
 - Part of SYSTEM hive
 - List of files
 - Executed flag
 - Timestamp
- Amcache
 - %WINDIR%\AppCompat\Programs\Amcache.hve
 - Same as shimcache but also stores hash of files

NTUSER & USRCLASS



- Each user has one of each
- User Activity
 - Files accessed
 - Searches
 - Network locations

Other Forensic Artifacts in Registry



- Shellbags
- RunMRU
- RecentDocs
- https://www.forensicswiki.org/wiki/Windows_Registry if you want to see more
- **Parsing registry files**
 - regripper
 - log2timeline
 - amcache parser
 - shimcache.py
 - Registry Explorer

Blue Team



- Limited use of changing registry directly for blue team
 - Add Take Ownership to right click for CNDs
- Mostly will change system and app settings through tools
 - Easier
 - Less risky

Red Team



- Need admin access to do anything fun with registry
- Persistence
- Anti-forensics

VT Summit - Steganography



- <https://github.com/DominicBreuker/stego-toolkit>
- Docker container with steg tools installed
 - Shared /data folder with host
- go.gmu.edu/steg
 - checklist for the majority of steg CTF challenges
- Two new TCTF steg challenges
 - Final Form
 - Thunderstruck

Proud Sponsors



Thank you to these organizations who give us their support:

BATTELLE

It can be done™

CRYPSIS™