MAGNET VIRTUAL SUMMIT 2023

Just Another (broken) Registry Parser

An open-source tool to read/recover registry Keys and Values from corrupted/broken registry hives

YOGESH KHATRI
Principal Investigator | CyberCX

#MVS2023

About me

- Yogesh Khatri - Principal Investigator @ CyberCX (Australia)
- 18 years in DFIR – Industry & Academia
  - Researcher, Developer, Reverse Engineer, Consultant, Professor
- Author, contributor and maintainer for several DFIR FOSS tools
  - mac_apt – macOS (and iOS) Artifact Parsing Tool
  - OneDrive log .ODL reader
  - UnifiedLog Reader
  - Spotlight parser
  - Others..

Why was this needed?

Ransomware affected hive, did not encrypt entire file..

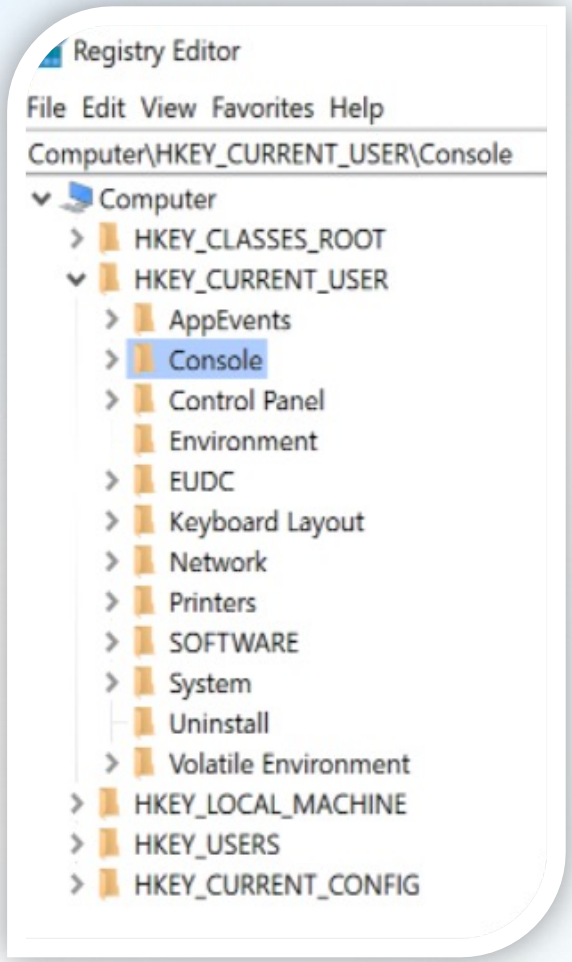
```
          0123456789ABCDEF0123456789ABCDEF
0000h: regf<1..<1.......................
0020h: .... ....P......\.?.?.\.c.:.\.u.
0040h: s.e.r.s.\.m.a.r.i.o.n.\.n.t.u.s.
0060h: e.r...d.a.t.....ã>‰.åxæ..Ýîû.,^Ù
0080h: ã>‰.åxæ..Ýîû.,^Ù....ä>‰.åxæ..Ýîû
00A0h: .,^Ùrmtm..Aðð.Ù.OfRg............
00C0h: ................................
```

Normal registry header

```
          0123456789ABCDEF0123456789ABCDEF
0000h: .EUþE?¿.Œµ¾S..-¶BM.1a¥¿Ê.™.¯ò.j.
0020h: .ð.Õ.TU¹=á}¥Ê.1±SüTå0£×\Lƒ.è.u.p
0040h: êèEƒÌ·.Õ.®Ê-p0ó"(¥é•šo^kVðBÃƒ±Å/
0060h: ä.îÀöt%r6ìpäõ?#ï‰¦."ã«à.éÕÂc.6°.
0080h: ß;ÃíÕàÃ...ë¹úÆ©-}ìê"tz¶.Ï×Ò.|.Ñµ
00A0h: .J,žœŽÃnÖ.†ß-ÖB×.ÈÄ©èÚR.Y^Ó©°.dM
00C0h: *.Âf×:(.Æ.õ"Lj¾.³¼-.¹ú9H.-[.X;!œ
```

Ransomware affected registry header

The Windows Registry



- Databases known as “hives”
- HKEY_LOCAL_USER stored in your profile at
  - C:\Users\<USER>\NTUSER.DAT
  - C:\Users\<USER>\AppData\Local\Microsoft\Windows\USRCLASS.DAT
- Most other hives at C:\Windows\System32\Config\
  - SOFTWARE
  - SYSTEM
  - SECURITY
  - SAM
  - ..

Registry Hive structure

Header “regf”

Data Block “hbin”

Data Block “hbin”

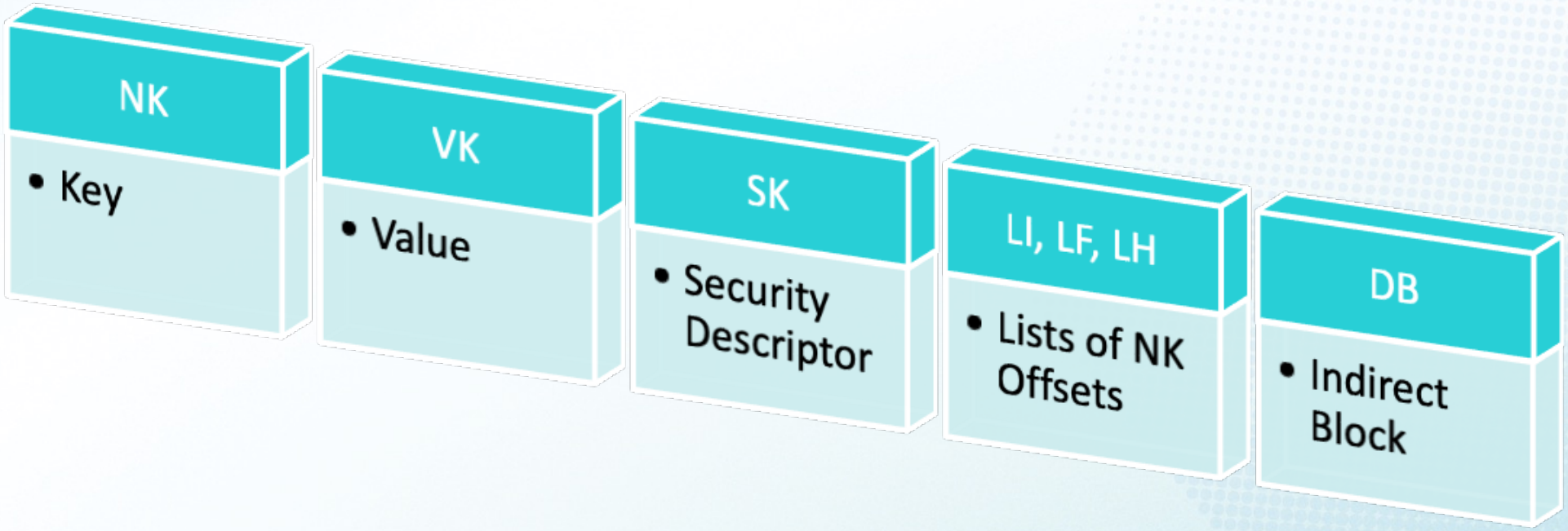
Data Block “hbin”

⋮

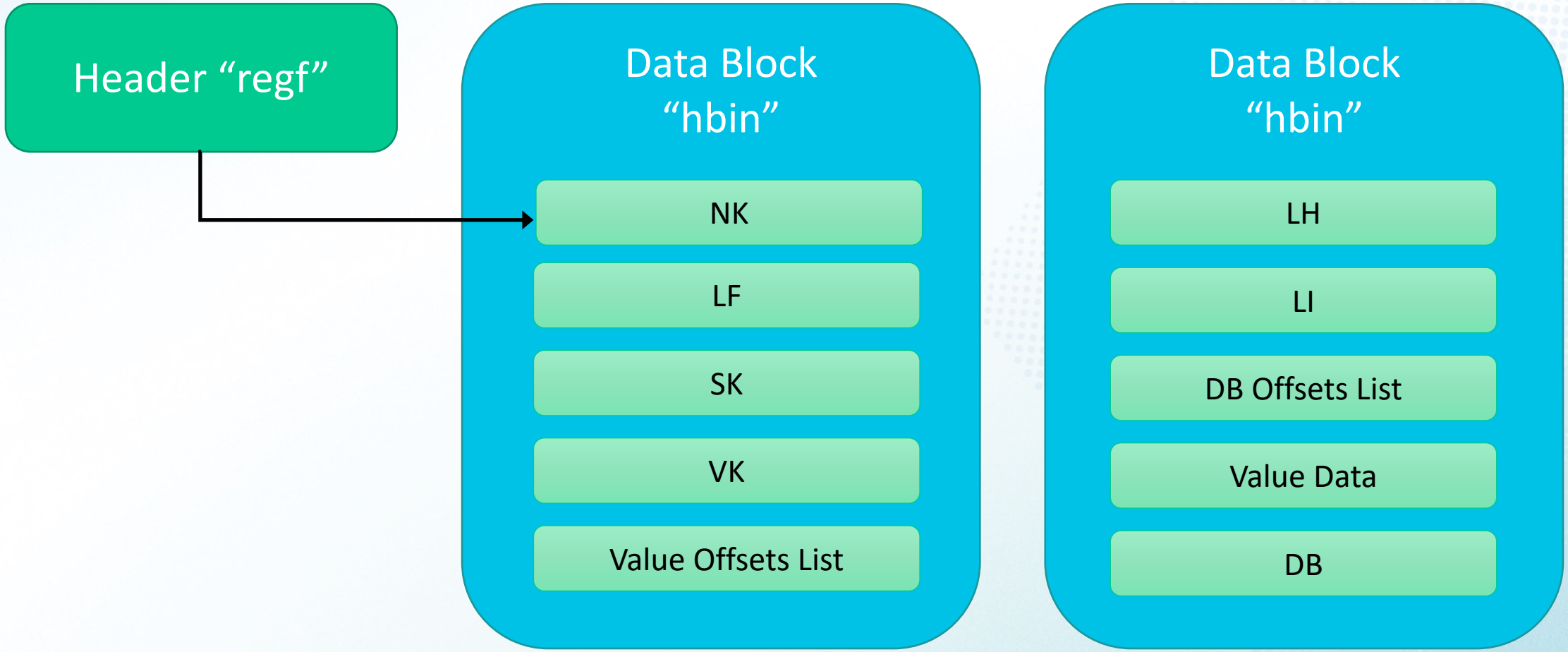
```
          0123456789ABCDEF0123456789ABCDEF
0000h: regf<1..<1.......................
0020h: .... ....P......\.?.?.\.c.:.\.u.
0040h: s.e.r.s.\.m.a.r.i.o.n.\.n.t.u.s.
0060h: e.r...d.a.t.....ã>‰.åxæ..Ýîû.,^Ù
0080h: ã>‰.åxæ..Ýîû.,^Ù....ä>‰.åxæ..Ýîû
00A0h: .,^Ùrmtm..Aðð.Ù.OfRg............
00C0h: ................................
```

```
          0123456789ABCDEF0123456789ABCDEF
1000h: hbin.............................
1020h: ¨ÿÿÿnk,..<1á±š×.....@............
1040h: Xx..ÿÿÿÿ....ÿÿÿÿ °..ÿÿÿÿ(.......
1060h: ................ROOT.... ÿÿÿnk .
1080h: <s6à±š×..... ..........ÿÿÿÿÿÿÿÿ
10A0h: ....0Þ..è...ÿÿÿÿ............f...
10C0h: !.......Environment. ...˜ÿÿÿnk .
```

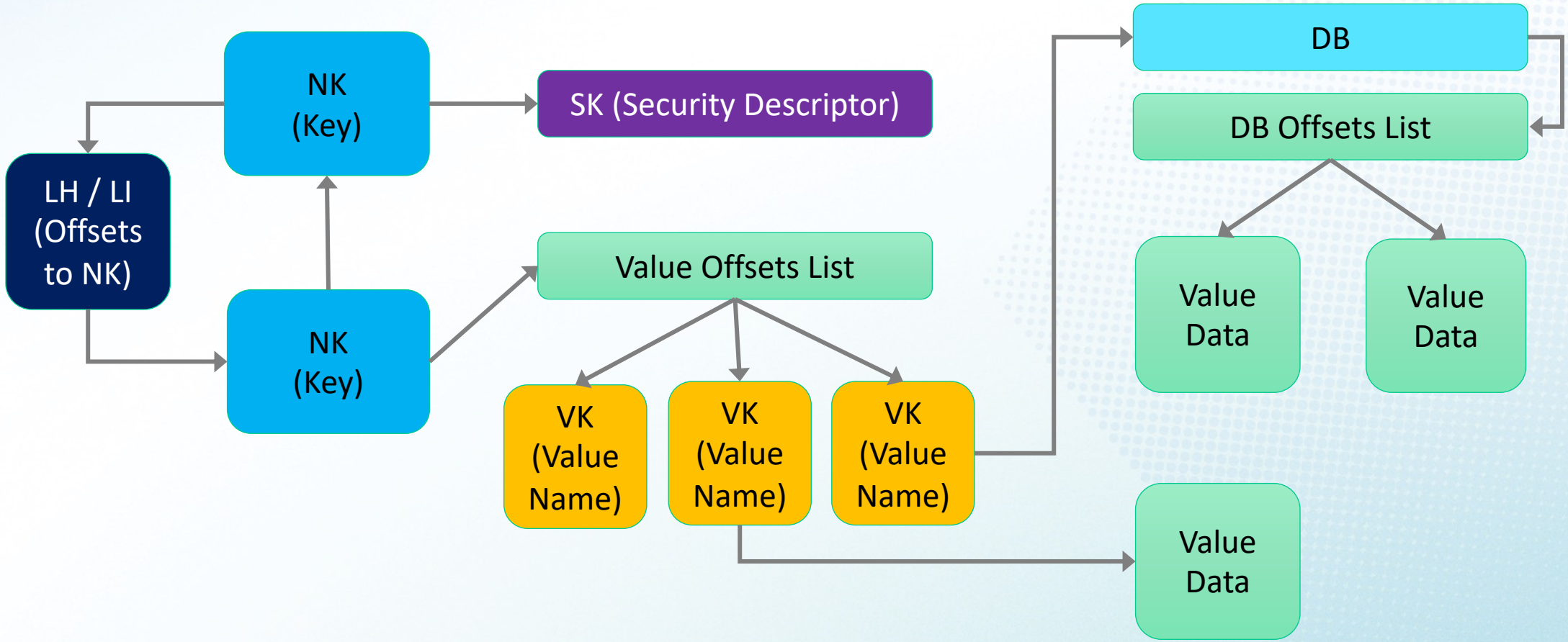
Registry objects stored in HBIN blocks/cells



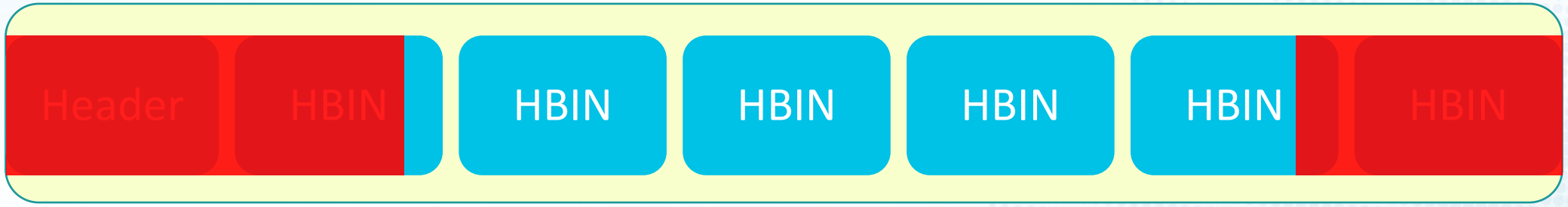
Hive structure



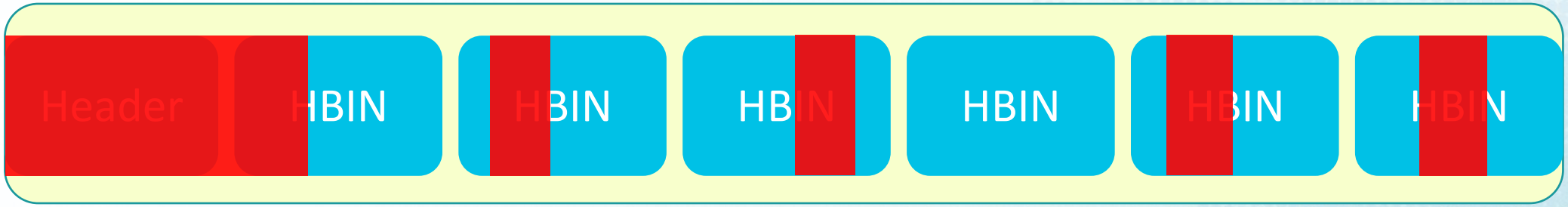
Relationships



Scenario - Ransomware



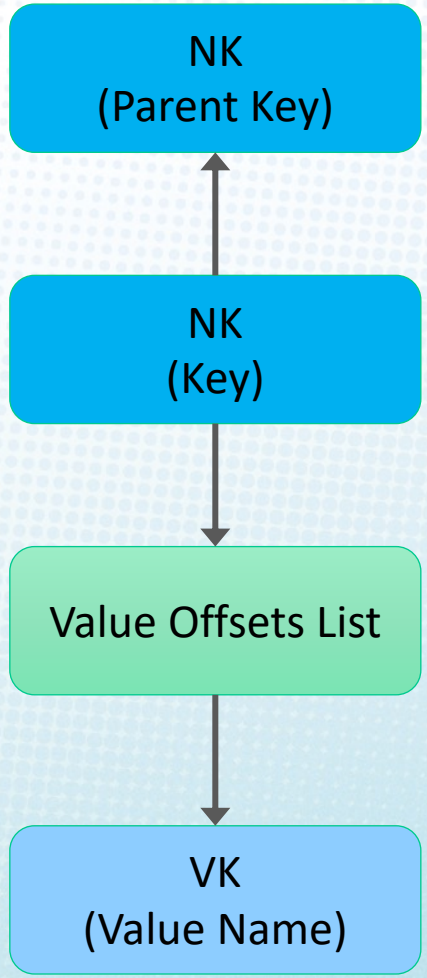
NTUSER.dat



NTUSER.dat

Recovering records

- Scan for NK (key names) and VK (value names) records
- Try to reconstruct key paths where possible
- Try to determine key for each value
  - Some Key-Value connections will be lost!
  - Some Values (name and/or data) may be lost!



Automate the process with *JARP*

- JARP will recover all possible records
  - Some records may be corrupted!
  - Avoids bad records by detecting null pointers or invalid offsets such as those greater than the hive file size
- Output is to console or SQLITE database
  - Console output can be filtered via keyword (normal or regex)
- Can un-ROT13 *UserAssist* keys (when successfully identified)

Demo

```
(env) ykhatri@SilverSurfer jarp % python jarp.py -h
usage: jarp.py [-h] [-o OUTPUT_PATH] [-p] [-n] [-f FILTER] [-r REGEX_FILTER] reg_path


  _  _  _  _
   //_//_//_/
(_// // \/    v 0.6.2 (c) Yogesh Khatri 2023 @swiftforensics

positional arguments:
  reg_path              Path to registry hive (file)

optional arguments:
  -h, --help            show this help message and exit
  -o OUTPUT_PATH, --output_path OUTPUT_PATH
                        Output file name and path (for sqlite output)
  -p, --print_to_screen
                        Print output to screen
  -n, --no_UA_decode    Do NOT decode rot13 for UserAssist (Default is to decode)
  -f FILTER, --filter FILTER
                        Filter keys and values. Eg: -f "UserAssist"
  -r REGEX_FILTER, --regex_filter REGEX_FILTER
                        Filter keys and values with regex. Eg: -f "User[a-zA-Z]+"

Just Another (broken) Registry Parser (JARP) was created to read
registry files that were partially corrupted and/or encrypted.
JARP will write all recovered keys & values to an sqlite
database and/or output recovered data on the console.

The filter options only apply to the console output (-p option).
```

References and Acknowledgement

- Eric Zimmerman for 010 template – *RegistryHive.bt*
- Willi Ballenthin for the ***python-registry*** project - *https://github.com/williballenthin/python-registry*

THANK YOU!

Download JARP here - https://github.com/ydkhatri/jarp

@SwiftForensics
yogesh@swiftforensics.com