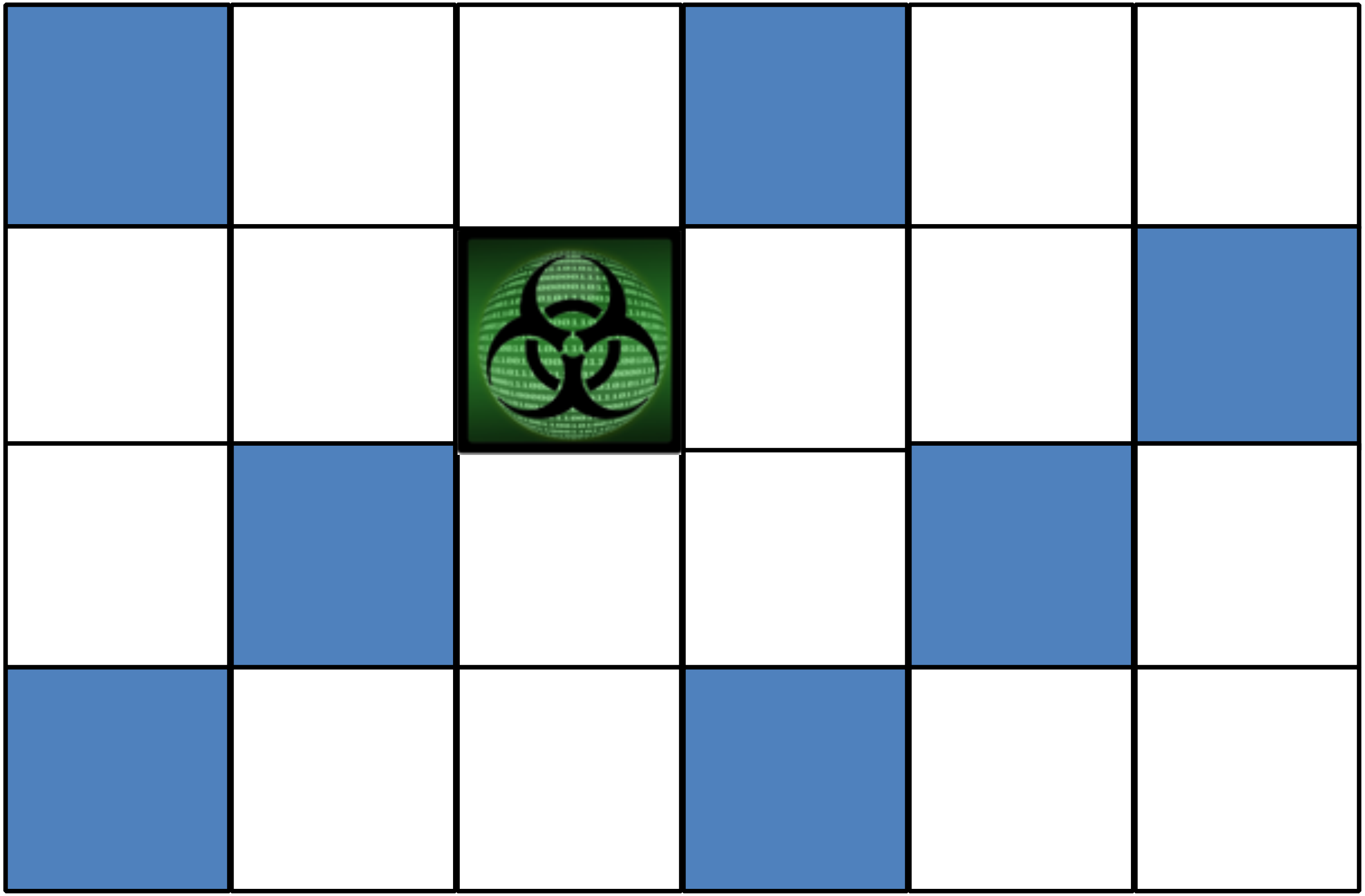
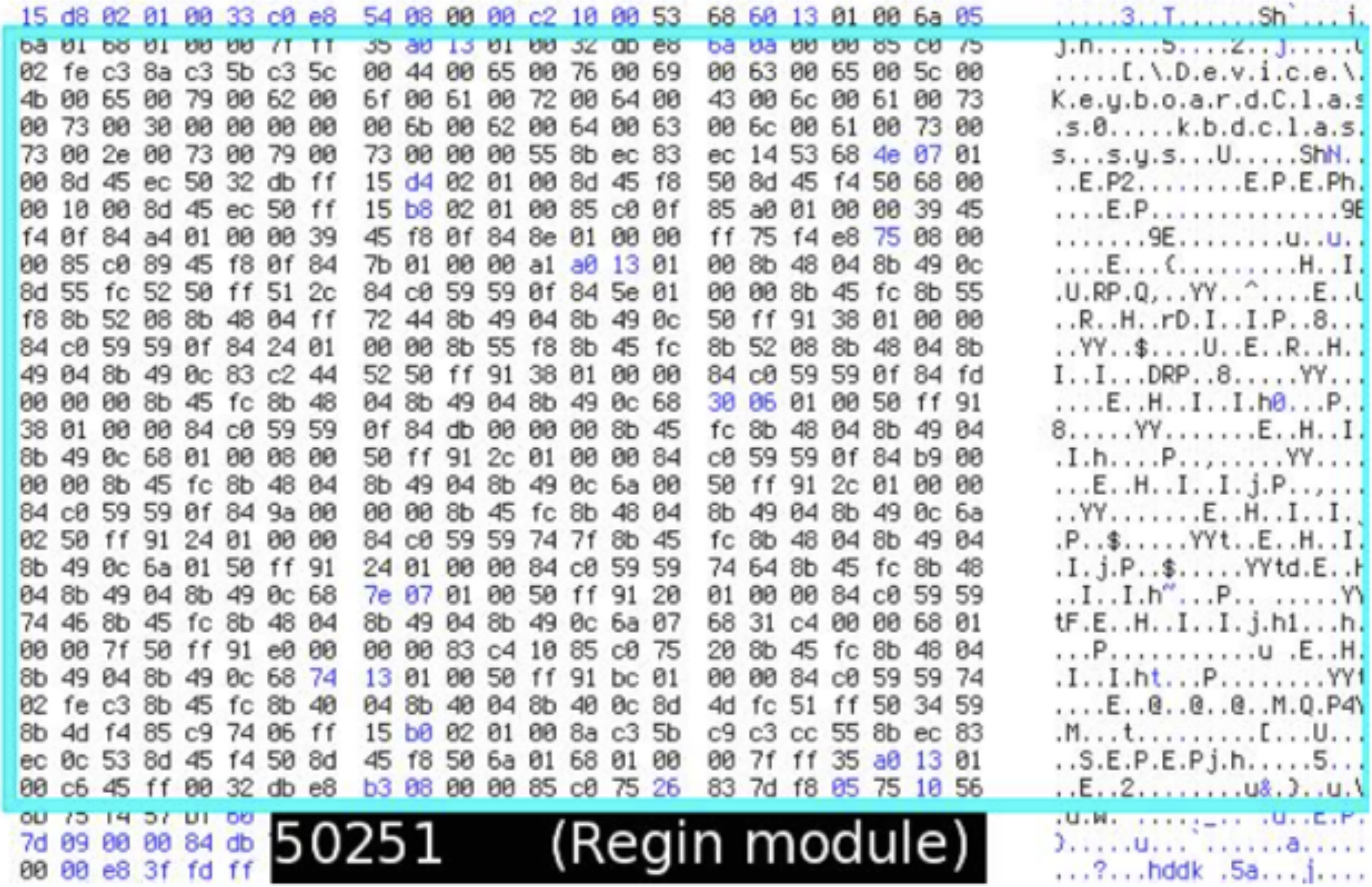
Malware Blocks

John Lukach

Needle-In-A-Haystack



Kaspersky Lab Analysis



```
15 d8 02 01 00 33 c0 e8  54 08 00 00 c2 10 00 53  68 60 13 01 00 6a 05       .....3..T......Sh`...i.
6a 01 68 01 00 00 7f ff  35 a0 13 01 00 32 db e8  6a 0a 00 00 85 c0 75       j.h.....5....2..j.....u
02 fe c3 8a c3 5b c3 5c  00 44 00 65 00 76 00 69  00 63 00 65 00 5c 00      .....[.\.D.e.v.i.c.e.\.
4b 00 65 00 79 00 62 00  6f 00 61 00 72 00 64 00  43 00 6c 00 61 00 73      K.e.y.b.o.a.r.d.C.l.a.s
00 73 00 30 00 00 00 00  00 6b 00 62 00 64 00 63  00 6c 00 61 00 73 00      .s.0.....k.b.d.c.l.a.s.
73 00 2e 00 73 00 79 00  73 00 00 00 55 8b ec 83  ec 14 53 68 4e 07 01      s...s.y.s...U.....ShN..
00 8d 45 ec 50 32 db ff  15 d4 02 01 00 8d 45 f8  50 8d 45 f4 50 68 00      ..E.P2.........E.P.E.Ph.
00 10 00 8d 45 ec 50 ff  15 b8 02 01 00 85 c0 0f  85 a0 01 00 00 39 45      ....E.P...............9E
f4 0f 84 a4 01 00 00 39  45 f8 0f 84 8e 01 00 00  ff 75 f4 e8 75 08 00      .......9E.........u..u..
00 85 c0 89 45 f8 0f 84  7b 01 00 00 a1 a0 13 01  00 8b 48 04 8b 49 0c      ....E...{.........H..I.
8d 55 fc 52 50 ff 51 2c  84 c0 59 59 0f 84 5e 01  00 00 8b 45 fc 8b 55      .U.RP.Q,..YY..^.....E..U
f8 8b 52 08 8b 48 04 ff  72 44 8b 49 04 8b 49 0c  50 ff 91 38 01 00 00      ..R..H..rD.I..I.P..8...
84 c0 59 59 0f 84 24 01  00 00 8b 55 f8 8b 45 fc  8b 52 08 8b 48 04 8b      ..YY..$....U..E..R..H..
49 04 8b 49 0c 83 c2 44  52 50 ff 91 38 01 00 00  84 c0 59 59 0f 84 fd      I..I...DRP..8.....YY...
00 00 00 8b 45 fc 8b 48  04 8b 49 04 8b 49 0c 68  30 06 01 00 50 ff 91      ....E..H..I..I.h0...P..
38 01 00 00 84 c0 59 59  0f 84 db 00 00 00 8b 45  fc 8b 48 04 8b 49 04      8.....YY.......E..H..I.
8b 49 0c 68 01 00 08 00  50 ff 91 2c 01 00 00 84  c0 59 59 0f 84 b9 00      .I.h....P..,.....YY....
00 00 8b 45 fc 8b 48 04  8b 49 04 8b 49 0c 6a 00  50 ff 91 2c 01 00 00      ...E..H..I..I.j.P..,...
84 c0 59 59 0f 84 9a 00  00 00 8b 45 fc 8b 48 04  8b 49 04 8b 49 0c 6a      ..YY.......E..H..I..I.j
02 50 ff 91 24 01 00 00  84 c0 59 59 74 7f 8b 45  fc 8b 48 04 8b 49 04      .P..$.....YYt..E..H..I.
8b 49 0c 6a 01 50 ff 91  24 01 00 00 84 c0 59 59  74 64 8b 45 fc 8b 48      .I.j.P..$.....YYtd.E..H
04 8b 49 04 8b 49 0c 68  7e 07 01 00 50 ff 91 20  01 00 00 84 c0 59 59      ..I..I.h~...P.. .....YY
74 46 8b 45 fc 8b 48 04  8b 49 04 8b 49 0c 6a 07  68 31 c4 00 00 68 01      tF.E..H..I..I.j.h1...h.
00 00 7f 50 ff 91 e0 00  00 00 83 c4 10 85 c0 75  20 8b 45 fc 8b 48 04      ...P...........u .E..H.
8b 49 04 8b 49 0c 68 74  13 01 00 50 ff 91 bc 01  00 00 84 c0 59 59 74      .I..I.ht...P.........YYt
02 fe c3 8b 45 fc 8b 40  04 8b 40 04 8b 40 0c 8d  4d fc 51 ff 50 34 59      .....E..@..@..@..M.Q.P4Y
8b 4d f4 85 c9 74 06 ff  15 b0 02 01 00 8a c3 5b  c9 c3 cc 55 8b ec 83      .M...t...........[...U..
ec 0c 53 8d 45 f4 50 8d  45 f8 50 6a 01 68 01 00  00 7f ff 35 a0 13 01      ..S.E.P.E.Pj.h.....5...
00 c6 45 ff 00 32 db e8  b3 08 00 00 85 c0 75 26  83 7d f8 05 75 10 56      ..E..2.........u&.}..u.V
8b 75 14 57 01 68                                                           .u.W. ....;_.. .u..E.P.
7d 09 00 00 84 db                                                           }.....u...`......a.....
00 00 e8 3f fd ff                                                           ...?...hddk .5a...j....
```

50251 (Regin module)

https://securelist.com/blog/research/68525/comparing-the-regin-module-50251-and-the-qwerty-keylogger/

bulk_extractor with hashdb

-S hashdb_mode =

none

import

scan

identified_blocks.txt

scan_expanded_hash

VirusShare.com

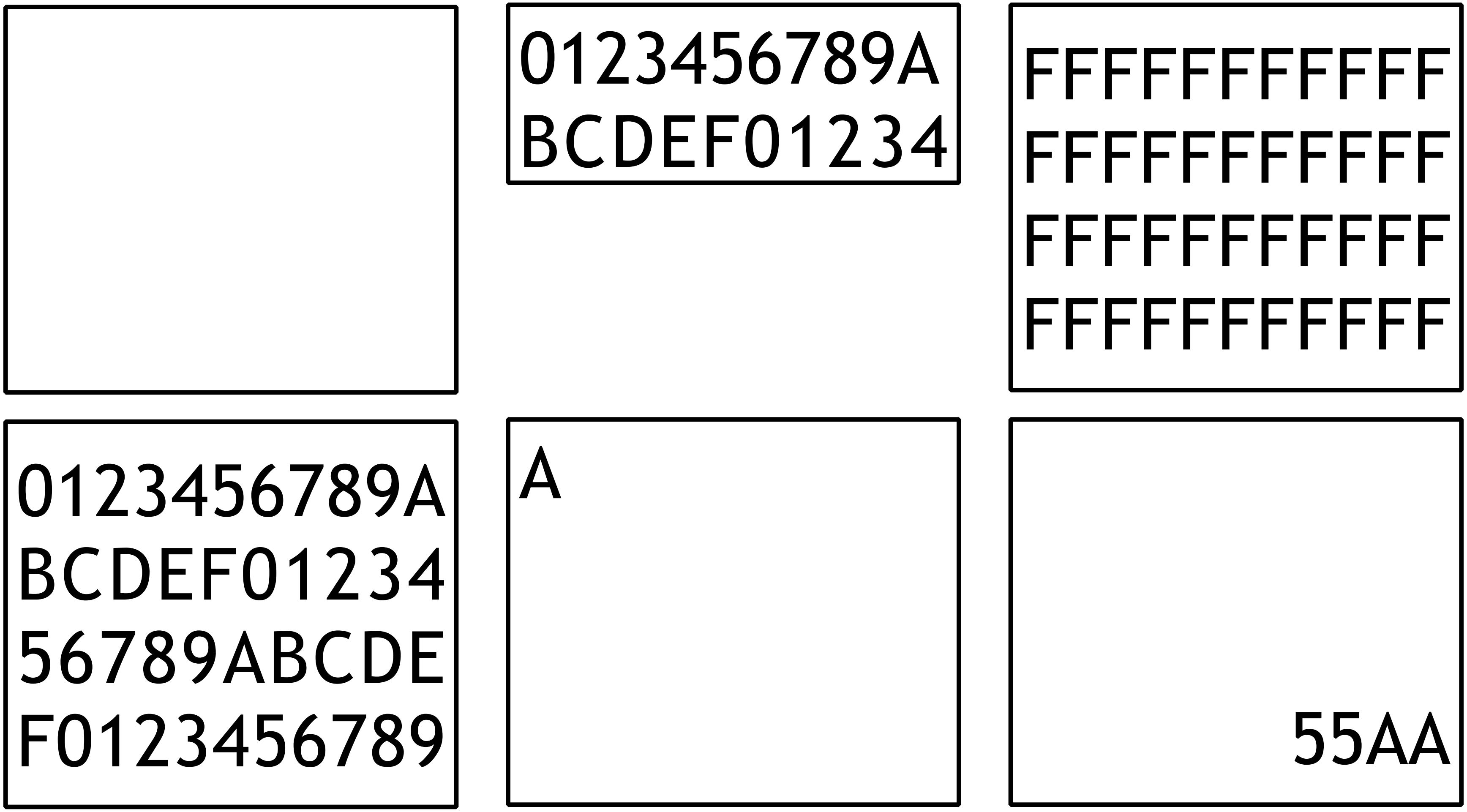
Cluster Blocks

1,296,092,861

Sector Blocks

9,391,656,074

Block Characteristics



0123456789A
BCDEF01234

FFFFFFFFFFF
FFFFFFFFFFF
FFFFFFFFFFF
FFFFFFFFFFF

0123456789A
BCDEF01234
56789ABCDE
F0123456789

A

55AA

NSRL Hash Set

File Hash	Block Hash	Index #
File Hash	Block Hash	Index #
File Hash	Block Hash	Index #

`http://nsrl.nist.gov/ftp/MD5B512/`

Bro

```
@load base/files/extract
@load base/files/hash

const block_size = 4096;

event file_state_remove(f: fa_file){
   local i = 0;
   while ( i < f$seen_bytes){
      print md5($bof_buffer[i:block_size]);
      i = i + block_size;
   }
}
```

FileBlock.Info

bulk_extractor module

- --blocks
- --view
- --list

https://github.com/jblukach/FileBlock.Info

Thanks!!

@FileBlocks