The Art of Binary Diffing
or
how to find 0-dayz for free

Nikita Tarakanov

ZeroNights 0x02, Moscow

#WhoAmI

- Crazy
- Fucking
- Wild
- Russian

Agenda

- Intro
- Overview of problem(s) of Binary Diffing
- Overview of differs
- Dude, so how to find 0-dayz???
- Conclusion
- Q&A

Intro

- 1dayz – what for?

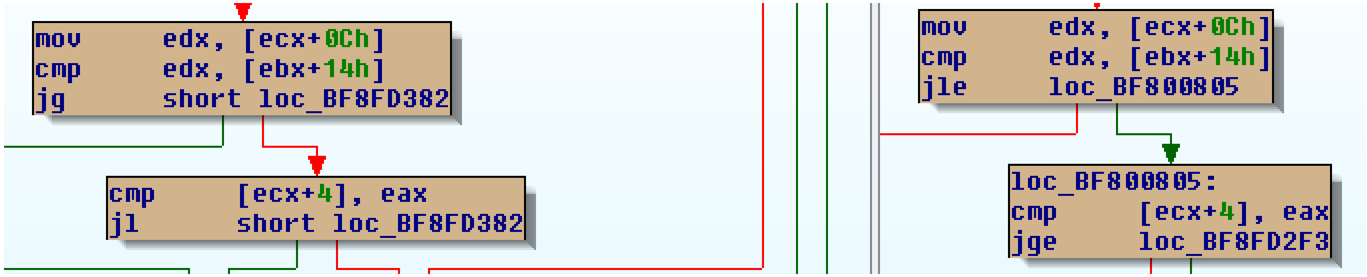
- 0dayz FTW!

Problem(s) of Binary Diffing

- Asm instructions are not atomic
- Different architectures
- Different compilers(even compiling options)
- Graph isomorphism – NP-full

Binary Diffing Sucks

- Sucks



```
mov     edx, [ecx+0Ch]
cmp     edx, [ebx+14h]
jg      short loc_BF8FD382
```

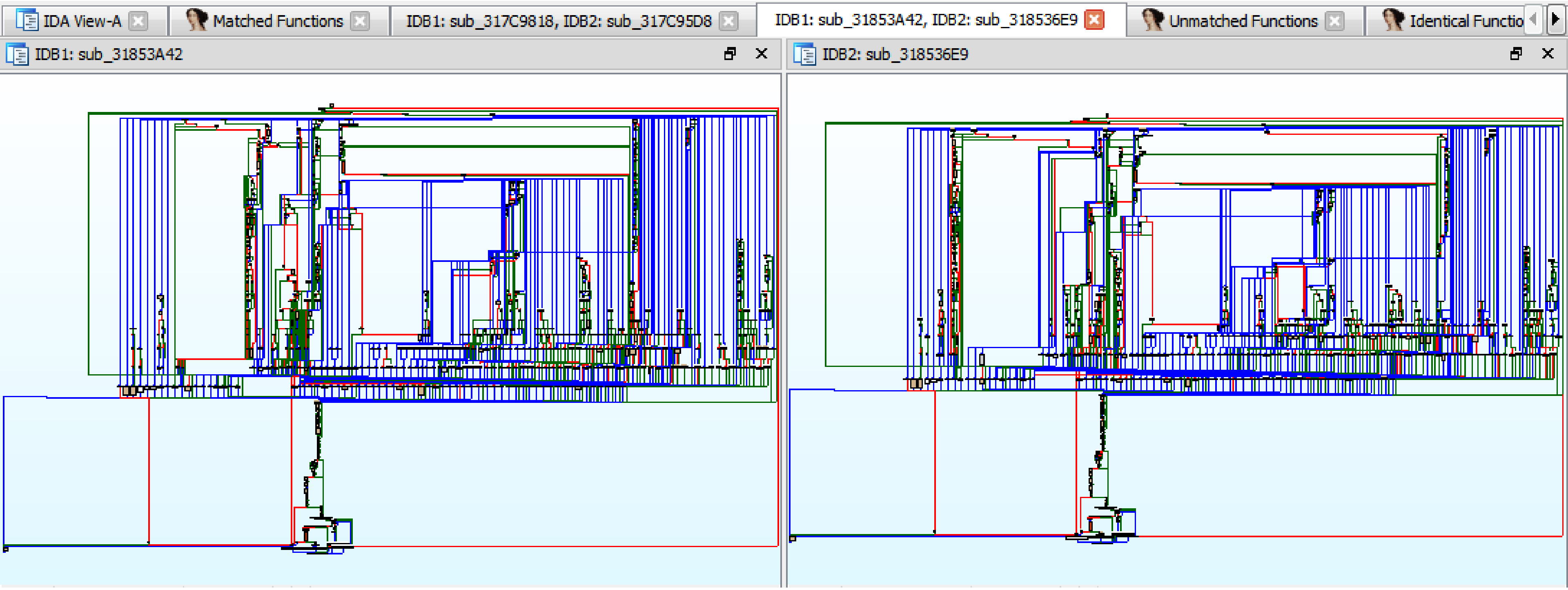
```
cmp     [ecx+4], eax
jl      short loc_BF8FD382
```

```
mov     edx, [ecx+0Ch]
cmp     edx, [ebx+14h]
jle     loc_BF800805
```

```
loc_BF800805:
cmp     [ecx+4], eax
jge     loc_BF8FD2F3
```

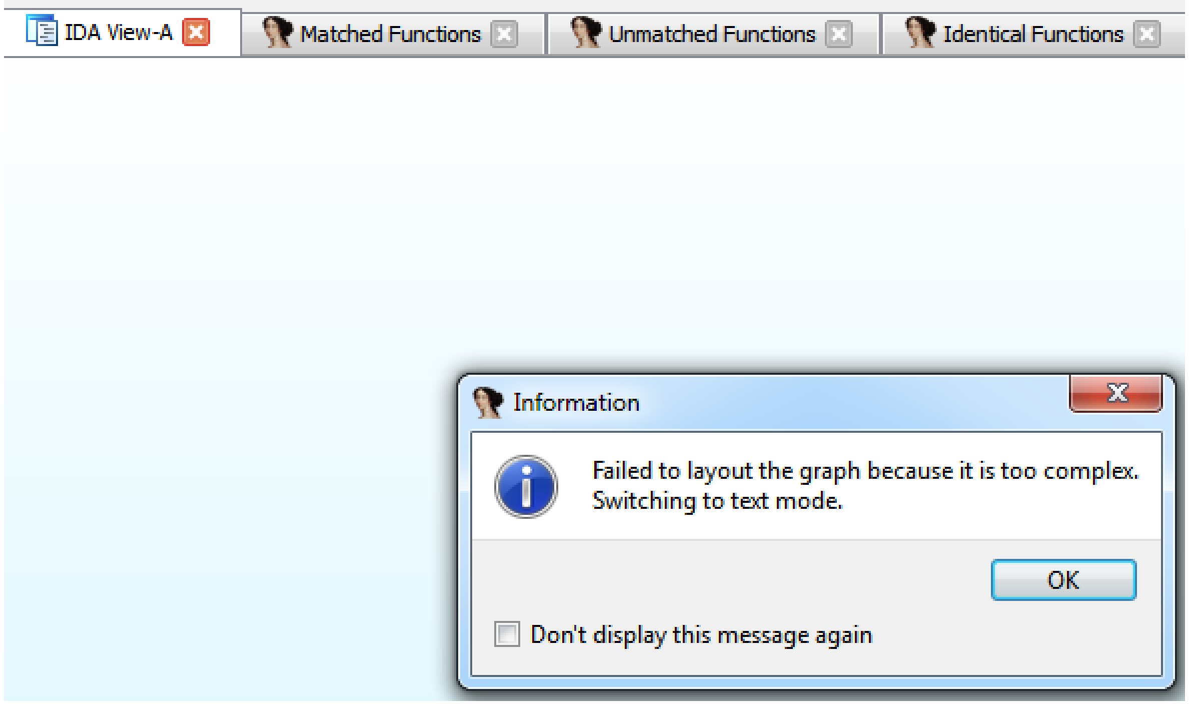
Binary Diffing Sucks

- Sucks



Binary Diffing Sucks

- Nope, it really SUCKS



Failed to layout the graph because it is too complex.
Switching to text mode.

Lets diff the differs!

Turbodiff

- Own graph implementation
- Special algo for unrecognized functions
- Basic algo
- Uses graphview
- Sucks

PatchDiff

- Several graph diffing algos
- Uses IDA graph GUI
- Sucks

BinDiff(out of scope)

- A lot graph diffing algos(Customizing)
- Own IL
- Own graph diffing GUI
- Costs money – Sucks
- Sucks

Dude!

So how to find

0dayz???

Idea №1

- Security fix is a pattern
- Sometime it’s even new type of vuln
- Patterns -> Knowledge base

Idea №2

- What about diffing software version N vs N+1
- Adobe Reader 10.X vs 11
- Windows 7 vs 8
- This is fount of 0-dayz!
- Nope, it’s not ½ dayz!

Diffing different versions

- A lot of noise
- How to define security fix?
- Simple Patters: jnb->jb, strcpy -> strncpy etc
- VSA
- Construct dataflow

#lulz

- Win32k.sys 0day
- Was
- Dropped
- On
- This
- slide

Conclusion

- Vendors don’t patch old versions

- This is Pizdets

Q&A

- Thanks You!
- @NTarakanov