

---

---

---

---

---



# Stage 1 (Setup)

RegExp: target

0x.....<sid>	0x00000000
some pointer	0xffff00000000...
0x00000000	0x00000000
0x00000000	0x00000000
⋮	

Confuse Array

0x.... <sid>	0x <bf-pointer>
0x00000000...	0x <some pointers>
0x0000...	0x00000000...
⋮	

...	stuff	2	p(13.3?)	p(13.3?)	...
-----	-------	---	----------	----------	-----

Containers

above

above-above

0x.....c7d3	0x00000000
0xffff0000...	0xffff0000...
0xffff0000...	0xffff0000...
0xffff0000...	0xffff0000...
0x.....c7d3	0x00000000
0xffff0000...	0xffff0000...
0xffff0000...	0xffff0000...
0xffff0000...	0xffff0000...
0x.....c7d3	0x00000000
0xffff0000...	0xffff0000...
0xffff0000...	0xffff0000...
0xffff0000...	0xffff0000...

Meta content Object Butterfly Code Pointer

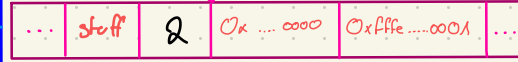
1. target[1] = 1;
2. Set RegExp proto to:
  - { has: function() {
  - confuse[1] = container;
  - }
  - } target

## Stage 2

0x ..... <sid>	0x <bf pointer>
some pointer	0x fffe 00000000 ...
0x 00000000	0x 00000000
0x 00000000	0x 00000000
⋮	

Confuse Array

0x .... <sid>	0x <bf-pointer>
0x 00000000 ...	0x <some pointers>
0x 0000 ...	0x 00 0000 ...
⋮	



Containers

0x ..... c7d3	0x 00000000
0x fffe 00000 ...	0x fffe 00000 ...
0x fffe 00000 ...	0x fffe 00000 ...
0x fffe 00000 ...	0x fffe 00000 ...
0x ..... c7d3	0x 00000000
0x fffe 00000 ...	0x fffe 00000 ...
0x fffe 00000 ...	0x fffe 00000 ...
0x fffe 00000 ...	0x fffe 00000 ...
0x ..... c7d3	0x 00000000
0x fffe 00000 ...	0x fffe 00000 ...
0x fffe 00000 ...	0x fffe 00000 ...
0x fffe 00000 ...	0x fffe 00000 ...

above

above-above

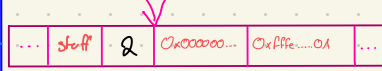


Meta content Object Butterfly Code Pointer

# Stage 3.1

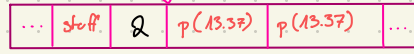
target

0x.....<sid>	0x <bf pointer>
some pointer	0x fffe 00000000 ...
0x00000000	0x00000000
0x00000000	0x00000000
⋮	



Confuse Array

0x... <sid>	0x <bf-pointers>
0x00000000...	0x <some pointers>
0x00000000...	0x00000000...
⋮	



u32 = new UInt32Array(4)

0x... <sid>	0x000000000000
data pointer	0x000000000004
0x00000000...	0x00000000...
⋮	

0x00000000 0000	0x00000000
0x00000000 00	0x00000000 00

Containers

0x.....c7d3	0x00000000
0x fffe 00000000...	0x fffe 00000000...
0x fffe 00000000...	0x fffe 00000000...
0x fffe 00000000...	0x fffe 00000000...
0x.....c7d3	0x00000000
0x fffe 00000000...	0x fffe 00000000...
0x fffe 00000000...	0x fffe 00000000...
0x fffe 00000000...	0x fffe 00000000...
0x.....c7d3	0x00000000
0x fffe 00000000...	0x fffe 00000000...
0x fffe 00000000...	0x fffe 00000000...
0x fffe 00000000...	0x fffe 00000000...

above

above\_above

Meta content Object Butterfly Code Pointer

# Stage 3.2

target

0x.....<sid>	0x <bf pointer>
some pointer	0x fffe 00000000 ...
0x00000000	0x00000000
0x00000000	0x00000000
⋮	



Containers

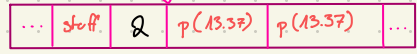
0x ..... c7d3	0x00000000
0x fffe 00000000 ...	0x fffe 00000000 ...
0x fffe 00000000 ...	0x fffe 00000000 ...
0x fffe 00000000 ...	0x fffe 00000000 ...
0x ..... c7d3	0x00000000
0x fffe 00000000 ...	0x fffe 00000000 ...
0x fffe 00000000 ...	0x fffe 00000000 ...
0x fffe 00000000 ...	0x fffe 00000000 ...
0x ..... c7d3	0x00000000
0x fffe 00000000 ...	0x fffe 00000000 ...
0x fffe 00000000 ...	0x fffe 00000000 ...
0x fffe 00000000 ...	0x fffe 00000000 ...

above

above..above

Confuse Array

0x... <sid>	0x <bf-pointers>
0x00000000 ...	0x <some pointers>
0x00000000 ...	0x00000000 ...
⋮	



u32

0x... <sid>	0x <bf-pointers>
some pointer	0x00002000000004
junk	junk
⋮	

f64 = new Float64(u32.buffer)

0x... <sid>	0x <bf-pointers>
some pointer	0x00002000000002
0x00000000	0x00000000
⋮	

0x00000000 0000	0x00000000
0x00000000 00	0x00000000

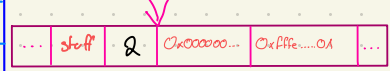


# Stage 4

Containers

target

0x.....<sid>	0x <bf pointer>
some pointer	0x fffe 00000000 ...
0x00000000	0x00000000
0x00000000	0x00000000
⋮	



0x ..... c7d3	0x00000000
0x fffe 00000000 ...	0x fffe 00000000 ...
0x fffe 00000000 ...	0x fffe 00000000 ...
0x fffe 00000000 ...	0x fffe 00000000 ...
0x ..... c7d3	0x00000000
0x fffe 00000000 ...	0x fffe 00000000 ...
0x fffe 00000000 ...	0x fffe 00000000 ...
0x fffe 00000000 ...	0x fffe 00000000 ...
0x ..... c7d3	0x00000000
0x fffe 00000000 ...	0x fffe 00000000 ...
0x fffe 00000000 ...	0x fffe 00000000 ...
0x fffe 00000000 ...	0x fffe 00000000 ...

above

above above

Confuse Array

0x.... <sid>	0x <bf-pointers>
0x00000000 ...	container + 0x10
0x00000000 ...	0x00000000 ...
⋮	



v32

0x.... <sid>	0x <bf-pointers>
some pointer	0x00002000000004
junk	junk
⋮	

f64

0x.... <sid>	0x <bf-pointers>
some pointer	0x00002000000002
0x00000000	0x00000000
⋮	

0x00000000 0000	0x00000000
0x00000000 0000	0x00000000 0000



1. JIT the victim
2. Trigger the type confusion
3. shift confusion's pointer to container by 0x10

# Stage 5.1

Containers

target

0x.....<sid>	0x <bf pointer>
some pointer	0x fffe 00000000 ...
0x00000000	0x00000000
0x00000000	0x00000000
⋮	

...	stuff	2	0x00000000	0x fffe.....01	...
-----	-------	---	------------	----------------	-----

Confuse Array

0x.... <sid>	0x <bf-pointers>
0x00000000 ...	container + 0x10
0x00000000 ...	0x00000000 ...
⋮	

...	stuff	2	p(13.37)	p(13.37)	...
-----	-------	---	----------	----------	-----

v32

0x.... <sid>	0x <bf-pointers>
some pointer	0x00002000000004
junk	junk
⋮	

f64

0x.... <sid>	0x <bf-pointers>
some pointer	0x00002000000002
0x00000000	0x00000000.00
⋮	

Fake obj

0x.....c7d3	0x00000000
↑ copy of this sid	0x fffe 00000000 ...
0x fffe 00000000 ...	0x fffe 00000000 ...
0x fffe 00000000 ...	0x fffe 00000000 ...
0x.....sid	<bf-pointers>
0x fffe 00000000 ...	0x fffe 00000000 ...
0x fffe 00000000 ...	0x fffe 00000000 ...
0x fffe 00000000 ...	0x fffe 00000000 ...
0x.....c7d3	0x00000000
0x fffe 00000000 ...	0x fffe 00000000 ...
0x fffe 00000000 ...	0x fffe 00000000 ...
0x fffe 00000000 ...	0x fffe 00000000 ...

above

...	1	p(13.37)	...
-----	---	----------	-----

above\_above

1. Allocate a butterfly for above\_container to overwrite later

0x00000000.00.00	0x00000000
0x00000000.00	0x00000000.00

...	data pointer	0x00000000	data pointer	0x00000000	...
-----	--------------	------------	--------------	------------	-----

# Stage 5.2

target

0x.....<sid>	0x <bf pointer>
some pointer	0x fffe 00000000 ...
0x00000000	0x00000000
0x00000000	0x00000000
⋮	

...	stuff	2	0x00000000	0x fffe.....01	...
-----	-------	---	------------	----------------	-----

Confuse Array

0x.... <sid>	0x <bf-pointers>
0x00.0000 ...	0x fffe 00000000 ...
0x0000 ...	0x00.0000 ...
⋮	

...	stuff	2	p(13.37)	p(13.37)	...
-----	-------	---	----------	----------	-----

v32

0x.... <sid>	0x <bf-pointers>
some pointer	0x000200000004
junk	junk
⋮	

f64

0x.... <sid>	0x <bf-pointers>
some pointer	0x000200000002
0x00000000	0x00000000
⋮	

Containers

Fake obj

container.a  
above

above.above

0x.....c7d3	0x00000000
↑ copy of this sid	0x fffe 00000000 ...
0x fffe 00000000 ...	0x fffe 00000000 ...
0x fffe 00000000 ...	0x fffe 00000000 ...
0x.....sid	fake Butterfly
0x fffe 00000000 ...	0x fffe 00000000 ...
0x fffe 00000000 ...	0x fffe 00000000 ...
0x fffe 00000000 ...	0x fffe 00000000 ...
0x.....c7d3	0x00000000
0x fffe 00000000 ...	0x fffe 00000000 ...
0x fffe 00000000 ...	0x fffe 00000000 ...
0x fffe 00000000 ...	0x fffe 00000000 ...

1. Overwrite above\_container's butterfly to point to itself  
container.f = above\_container

2. remove reference to container from confuse

3. run GC

0x00000000 00.00	0x00000000
0x00000000 00	0x00000000 00

...	data pointer	0x00000000	data pointer	0x00000000	...
-----	--------------	------------	--------------	------------	-----

Meta content Object Butterfly Code Pointer