2. BuildStubThumb

```
ARM64 mode
_shellcode_stub_start:
SUB     SP, SP, #0x20
MRS     X0, NZCV
STR     X0, [SP, #0x10]
......
MOV     X0, SP
LDR     X3, 8
B       12
[_hookstub_function
_addr_ss]
BLR     X3
LDR     X0, [SP, #0x100]
MSR     NZCV, X0
LDP     X0, X1, [SP]
.....
STP     X1, X0, [SP, #-0x10]
LDR     X0, 8
B       12
[_old_function
_addr_s]
BR      X0
```

```
ARM64 mode
User’ s hook
stub function
```

2

1

4. RebuildHookTargetThumb

```
ARM64 mode
LDR     W9, [X8]
ADD     W9, W9, #1
STP     X1, X0, [SP, #-0x10]
LDR     X0, 8
BR      X0
[_shellcode_stub
_start](64 bit)
LDR     X0, [SP, #-0x8]
LDR     X0, [SP, #0x20 + var_10]
BL      ._ZN7_JNIEnv12NewString...

target_addr : LDR X0, [SP, #-0x8]
```

4

```
ARM64 mode          3
_old_function_addr:
STR     W9, [X8]
LDR     W9, [X8]
CMP     W9, #0xA
B.LS    0x1C ; [target_addr]
ADRP    X8, 0 ; “Enough”
ADD     X1, X8, #0x68C ; “Enough”
STP     X1, X0, [SP, #-0x10]
LDR     X0, 8
BR      X0
[HOOK_ADDR
 + 20Byte](64 bit)
```

1. InitThumbHookInfo

```
ARM64 mode
LDR     W9, [X8]
ADD     W9, W9, #1
STR     W9, [X8]
LDR     W9, [X8]
CMP     W9, #0xA
B.LS    0x1C ; [target_addr]
ADRP    X8, 0 ; “Enough”
ADD     X1, X8, #0x68C ; “Enough”
LDR     X0, [SP, #0x20 + var_10]
BL      ._ZN7_JNIEnv12NewString...

target_addr : ADRP X8, 0
```

3. BuildOldFunctionThumb

Fix

```
ARM64 mode
_old_function_addr:
STR     W9, [X8]
LDR     W9, [X8]
CMP     W9, #0xA
B.HI    0x30
LDR     X0, 8
B       12
[PAGE_VALUE
_ADDR](64 bit)
STP X0, X0, [SP, -0x10]
LDR X0, 12
BR X0
B       8
[target_
addr](64 bit)
LDR     X0, 8
B       12
[PAGE_VALUE
_ADDR](64 bit)
ADD     X1, X8, #0x68C ; “Enough”
STP     X1, X0, [SP, #-0x10]
LDR     X0, 8
BR      X0
[HOOK_ADDR
 + 20Byte](64 bit)
```