shellcode\_stub\_start:

ARM64 mode

```
SUB
                                                             SP, SP, #0x20
                                                     MRS
                                                             X0, NZCV
                                                             X0, [SP, #0x10]
                                                     STR
                                                     MOV
                                                             X0, SP
          ARM64 mode
                                                     LDR
                                                             X3, 8
          User's hook
                                                     В
                                                             12
          stub function
                                                     [_hookstub_function
                                                     _addr_ss]
                                                     BLR
                                                             X3
                               1
                                                             X0, [SP, #0x100]
                                                     LDR
                                                     MSR
                                                             NZCV, X0
                                                     LDP
                                                             X0, X1, [SP]
   4. RebuildHookTargetThumb
                                                     STP
                                                             X1, X0, [SP, #-0x10]
                                                     LDR
                                                             X0, 8
ARM64 mode
                                                     В
                                                             12
LDR
        W9, [X8]
                                                     [_old function
        W9, W9, #1
ADD
                                                     _addr_s]
        X1, X0, [SP, #-0x10]
STP
                                                             X0
                                                     BR
LDR
        X0, 8
BR
        X0
                                                     ARM64 mode
[_shellcode stub
                                                     _old_function_addr:
_start](64 bit)
                                                     STR
                                                             W9, [X8]
LDR
        X0, [SP, #-0x8] •
                                                     LDR
                                                             W9, [X8]
        X0, [SP, #0x20 + var_10]
LDR
                                                     CMP
                                                             W9, #0xA
        ._ZN7_JNIEnv12NewString...
BL
                                                     B.LS
                                                             0x1C ; [target_addr]
                                                     ADRP
                                                             X8, 0; "Enough"
target_addr: LDR X0, [SP, #-0x8]
                                                             X1, X8, #0x68C; "Enough"
                                                     ADD
                                                             X1, X0, [SP, #-0x10]
                                                     STP
  1. InitThumbHookInfo
                                                     LDR
                                                             X0, 8
                                                     BR
                                                             X0
  ARM64 mode
                                                     [HOOK_ADDR
  LDR
           W9, [X8]
                                                      + 20Byte](64 bit)
  ADD
           W9, W9, #1
  STR
           W9, [X8]
                                                    3.\,Build Old Function Thumb
           W9, [X8]
  LDR
  CMP
           W9, #0xA
```

**B.LS** 

**ADRP** 

ADD

LDR

BL

0x1C ; [target\_addr]

X1, X8, #0x68C; "Enough"

.\_ZN7\_JNIEnv12NewString...

X0, [SP, #0x20 + var 10]

X8, 0; "Enough"

target addr: ADRP X8, 0

```
ARM64 mode
old function addr:
STR
        W9, [X8]
LDR
        W9, [X8]
CMP
        W9, #0xA
B.HI
        0x30
LDR
        X0, 8
        12
[PAGE VALUE
ADDR](64 bit)
STP X0, X0, [SP, -0x10]
LDR X0, 12
BR X0
В
[target
addr](64 bit)
LDR
        X0, 8
В
[PAGE VALUE
_ADDR](64 bit)
        X1, X8, #0x68C; "Enough"
ADD
        X1, X0, [SP, #-0x10]
STP
LDR
        X0, 8
BR
        X0
[HOOK ADDR
+ 20Byte](64 bit)
```