

Static analysis

Objective c method:

-[_TtC7DVIA_v232JailbreakDetectionViewController jailbreakTest1Tapped:]

When 'Jailbreak Test 1' gets tapped, the following swift function is called:

__T07DVIA_v232JailbreakDetectionViewControllerC20jailbreakTest1TappedyypF

```

-[_TtC7DVIA_v232JailbreakDetectionViewController jailbreakTest1Tapped:]      // -[DVIA_v2.JailbreakDetectionViewController jailbreakTest1Tapped:]
0000000100192cb0      sub     sp, sp, #0x60                ; Objective C Implementation defined at 0x1003f8b18 (instance method), DATA
0000000100192cb4      stp     x20, x19, [sp, #0x40]
0000000100192cb8      stp     fp, lr, [sp, #0x50]
0000000100192cbc      add     fp, sp, #0x50
0000000100192cc0      str     x0, [sp, #0x50 + var_38]
0000000100192cc4      mov     x0, x2                    ; argument "instance" for method imp___stubs__swift_unknownRetain
0000000100192cc8      str     x1, [sp, #0x50 + var_40]
0000000100192ccc      str     x2, [sp, #0x50 + var_40]
0000000100192cd0      bl      imp___stubs__swift_unknownRetain    ; swift_unknownRetain
0000000100192cd4      ldr     x0, [sp, #0x50 + var_38]          ; argument "instance" for method imp___stubs__objc_retain
0000000100192cd8      bl      imp___stubs__objc_retain          ; objc_retain
0000000100192cdc      add     x8, sp, #0x20
0000000100192ce0      ldr     x1, [sp, #0x50 + var_40]
0000000100192ce4      str     x0, [sp, #0x50 + var_50]
0000000100192ce8      mov     x0, x1
0000000100192cec      bl      imp___stubs__T0s018_bridgeAnyObjectToB0yypXLSgF ; Swift._bridgeAnyObjectToAny(Swift.AnyObject?) -> Any
0000000100192cf0      add     x0, sp, #0x20              ; argument #1 for method __T07DVIA_v232JailbreakDetectionViewControllerC20jailbreakTest1TappedyypF
0000000100192cf4      ldr     x20, [sp, #0x50 + var_38]
0000000100192cf8      bl      __T07DVIA_v232JailbreakDetectionViewControllerC20jailbreakTest1TappedyypF ; DVIA_v2.JailbreakDetectionViewController.jailbreakTest1Tapped:()
0000000100192cfc      ldr     x0, [sp, #0x50 + var_38]          ; argument "instance" for method imp___stubs__objc_release
0000000100192d00      bl      imp___stubs__objc_release        ; objc_release
0000000100192d04      ldp     fp, lr, [sp, #0x50]
0000000100192d08      ldp     x20, x19, [sp, #0x40]
0000000100192d0c      add     sp, sp, #0x60
0000000100192d10      ret

```

Disassembly of the swift function:

```

__T07DVIA_v232JailbreakDetectionViewController20jailbreakTest1TappeddyppF: // DVIA_v2.JailbreakDetectionViewController.ja
0000000100192c10    sub     sp, sp, #0x60                                ; CODE XREF=_[TtC7DVIA_v232JailbreakDetectionViewController jailbrea
0000000100192c14    stp     x20, x19, [sp, #0x40]
0000000100192c18    stp     fp, lr, [sp, #0x50]
0000000100192c1c    add     fp, sp, #0x50
0000000100192c20    stur    x0, [fp, var_18]
0000000100192c24    stur    x20, [fp, var_20]
0000000100192c28    str     x20, [sp, #0x50 + var_28]
0000000100192c2c    str     x0, [sp, #0x50 + var_30]
0000000100192c30    bl      __T07DVIA_v213DVIAUtilitiesCMA                ; type metadata accessor for DVIA_v2.DVIAUtilities
0000000100192c34    adrp    x20, #0x1003a4000                               ; 0x1003a4708@PAGE
0000000100192c38    ldr     x20, [x20, #0x708]                             ; 0x1003a4708@PAGEOFF, _swift_isaMask_1003a4708,_swift_isaMask
0000000100192c3c    ldr     lr, [x0, #0x58]
0000000100192c40    ldr     x8, [sp, #0x50 + var_28]
0000000100192c44    ldr     x9, [x8]
0000000100192c48    ldr     x20, [x20]                                     ; _swift_isaMask
0000000100192c4c    and     x9, x9, x20
0000000100192c50    ldr     x9, [x9, #0x80]
0000000100192c54    mov     x20, x8
0000000100192c58    str     x0, [sp, #0x50 + var_38]
0000000100192c5c    str     lr, [sp, #0x50 + var_40]
0000000100192c60    blr     x9
0000000100192c64    ldr     x8, [sp, #0x50 + var_28]
0000000100192c68    str     w0, [sp, #0x50 + var_44]
0000000100192c6c    mov     x0, x8                                         ; argument "instance" for method imp__stubs_objc_retain
0000000100192c70    bl      imp__stubs_objc_retain                         ; objc_retain
0000000100192c74    ldr     x8, [sp, #0x50 + var_28]
0000000100192c78    ldr     x9, [sp, #0x50 + var_40]
0000000100192c7c    ldr     w10, [sp, #0x50 + var_44]
0000000100192c80    and     w11, w10, #0x1
0000000100192c84    str     x0, [sp, #0x50 + var_50]
0000000100192c88    mov     x0, x11
0000000100192c8c    mov     x1, x8
0000000100192c90    ldr     x20, [sp, #0x50 + var_38]
0000000100192c94    blr     x9
0000000100192c98    ldr     x0, [sp, #0x50 + var_30]                       ; argument #1 for method __swift_destroy_boxed_opaque_existential_0
0000000100192c9c    bl      __swift_destroy_boxed_opaque_existential_0    ; __swift_destroy_boxed_opaque_existential_0
0000000100192ca0    ldp     fp, lr, [sp, #0x50]
0000000100192ca4    ldp     x20, x19, [sp, #0x40]

```

Bypassing the said mechanism using objection:

```

....highAltitudehacks.DVIAswiftv2 on (iPhone: 12.5.6) [usb] # ios jailbreak disable
(agent) Registering job 588681. Type: ios-jailbreak-disable
....highAltitudehacks.DVIAswiftv2 on (iPhone: 12.5.6) [usb] # (agent) [588681] fileExistsAtPath: check for /Applications/Cydia.app was successful with: 0x1, marking it as fail
ed.
(agent) [588681] fileExistsAtPath: check for /bin/bash was successful with: 0x1, marking it as failed.
(agent) [588681] fileExistsAtPath: check for /usr/sbin/sshd was successful with: 0x1, marking it as failed.
(agent) [588681] fileExistsAtPath: check for /etc/apt was successful with: 0x1, marking it as failed.
(agent) [588681] canOpenURL: check for cydia://package/com.example.package was successful with: 0x1, marking it as failed.

```

Results:

