

loc\_182489c60

```
RSP = RSP + -0x8
@64[RSP + -0x8] = RBP

RSP = RSP + -0x8
@64[RSP + -0x8] = R15

RSP = RSP + -0x8
@64[RSP + -0x8] = R14

RSP = RSP + -0x8
@64[RSP + -0x8] = R13

RSP = RSP + -0x8
@64[RSP + -0x8] = R12

RSP = RSP + -0x8
@64[RSP + -0x8] = RSI

RSP = RSP + -0x8
@64[RSP + -0x8] = RDI

RSP = RSP + -0x8
@64[RSP + -0x8] = RBX

zf = FLAG_EQ_CMP(RSP, 0x68)
nf = FLAG_SIGN_SUB(RSP, 0x68)
pf = parity((RSP + -0x68) & 0xFF)
cf = FLAG_SUB_CF(RSP, 0x68)
of = FLAG_SUB_OF(RSP, 0x68)
af = ((RSP ^ 0x68) ^ (RSP + -0x68))[4:5]
RSP = RSP + -0x68

RBP = RSP + 0x60

@64[RBP] = 0xFFFFFFFFFFFFFFFE

RCX = 0x182489C84 + 0x113C29F

@64[RBP + 0xFFFFFFFFFFFFFFF0] = RCX

RCX = zeroExt_64(0x89F4)

zf = FLAG_EQ_CMP(RCX, -@64[RBP + 0xFFFFFFFFFFFFFFF0])
nf = FLAG_SIGN_SUB(RCX, -@64[RBP + 0xFFFFFFFFFFFFFFF0])
pf = parity((RCX + @64[RBP + 0xFFFFFFFFFFFFFFF0]) & 0xFF)
cf = FLAG_ADD_CF(RCX, @64[RBP + 0xFFFFFFFFFFFFFFF0])
of = FLAG_ADD_OF(RCX, @64[RBP + 0xFFFFFFFFFFFFFFF0])
af = ((RCX ^ @64[RBP + 0xFFFFFFFFFFFFFFF0]) ^ (RCX + @64[RBP + 0xFFFFFFFFFFFFFFF0]))[4:5]
RCX = RCX + @64[RBP + 0xFFFFFFFFFFFFFFF0]

]@64[RBP + 0xFFFFFFFFFFFFFFF8] = RCX

RCX = @64[RBP + 0xFFFFFFFFFFFFFFF8]

]R8 = zeroExt_64(@32[RCX + 0xFFFFFFFFFFE3A49])

RCX = 0x182489CA7 + 0xDCE9C

@64[RBP + 0xFFFFFFFFFFFFFFF8] = RCX

R9 = zeroExt_64(@32[0x182489CB2 + 0x114A7D2])

RCX = @64[segm(GS, 0x58)]

RCX = @64[RCX + R9 * 0x8

]R11 = 0x182489CC6 + 0x2A07D

R10 = 0xFFFFFFFFF2345A

zf = FLAG_EQ_CMP(R10, -@64[RBP + 0xFFFFFFFFFFFFFFF8])
nf = FLAG_SIGN_SUB(R10, -@64[RBP + 0xFFFFFFFFFFFFFFF8])
pf = parity((R10 + @64[RBP + 0xFFFFFFFFFFFFFFF8]) & 0xFF)
cf = FLAG_ADD_CF(R10, @64[RBP + 0xFFFFFFFFFFFFFFF8])
of = FLAG_ADD_OF(R10, @64[RBP + 0xFFFFFFFFFFFFFFF8])
af = ((R10 ^ @64[RBP + 0xFFFFFFFFFFFFFFF8]) ^ (R10 + @64[RBP + 0xFFFFFFFFFFFFFFF8]))[4:5]
R10 = R10 + @64[RBP + 0xFFFFFFFFFFFFFFF8]

]@64[RBP + 0xFFFFFFFFFFFFFFF8] = R11

R11 = 0xFFFFFFFFFD5FAB

zf = FLAG_EQ_CMP(R11, -@64[RBP + 0xFFFFFFFFFFFFFFF8])
nf = FLAG_SIGN_SUB(R11, -@64[RBP + 0xFFFFFFFFFFFFFFF8])
pf = parity((R11 + @64[RBP + 0xFFFFFFFFFFFFFFF8]) & 0xFF)
cf = FLAG_ADD_CF(R11, @64[RBP + 0xFFFFFFFFFFFFFFF8])
of = FLAG_ADD_OF(R11, @64[RBP + 0xFFFFFFFFFFFFFFF8])
af = ((R11 ^ @64[RBP + 0xFFFFFFFFFFFFFFF8]) ^ (R11 + @64[RBP + 0xFFFFFFFFFFFFFFF8]))[4:5]
R11 = R11 + @64[RBP + 0xFFFFFFFFFFFFFFF8]

]zf = FLAG_EQ_CMP((R8)[0:32], @32[RCX + 0x44])
nf = FLAG_SIGN_SUB((R8)[0:32], @32[RCX + 0x44])
pf = parity(((R8)[0:32] + -@32[RCX + 0x44]) & 0xFF)
cf = FLAG_SUB_CF((R8)[0:32], @32[RCX + 0x44])
of = FLAG_SUB_OF((R8)[0:32], @32[RCX + 0x44])
af = (((R8)[0:32] ^ @32[RCX + 0x44]) ^ ((R8)[0:32] + -@32[RCX + 0x44]))[4:5]

R11 = R11

IRDst = CC_S<=(nf, of, zf)?(loc_key_1, loc_182489ceb)
```

loc\_key\_1

```
R11 = R10
IRDst = loc_182489ceb
```

loc\_182489ceb

```
RIP = R11
IRDst = R11
```