<https://youtu.be/Yl-_F6b4hbg>

Infor:

10D50 – 8400 = X – B000

X = 13950

Add image base = 01013950 (50 39 01 01)

Text:

10D60 – 8400 = Y – B000

Y = 13960

Add image base = 01013960 (60 39 01 01)

Code:

New entry point:

10DA0 – 8400 + B000 = 139A0

Old\_entry\_point = jmp + 5 + R\_VA

0100739D = 000139A0 + image base + 14 + 5 + R\_VA

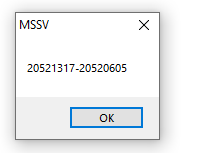
R\_VA = FFFF39E4 (E4 39 FF FF)

Payload

6A 00 68 50 39 01 01 68 60 39 01 01 6A 00 FF 15 68 12 00 01 E9 E4 39 FF FF

4D 00 53 00 53 00 56 00 (MSSV)

32 00 30 00 35 00 32 00 31 00 33 00 31 00 37 00 2D 00 32 00 30 00 35 00 32 00 30 00 36 00 30 00 35 00 (20521317-20520605)



Calc



Message BoxW 010011A8

Virtual addresse: 16000

Raw address: 13600

Graphical user interface, application

Description automatically generated

Address of entry point

Graphical user interface

Description automatically generated with low confidence

Info:

1BF70 – 13600 = X – 16000

X = 1E970

Add image base 0101E970 (70 E9 01 01)

Text:

1BF80 – 13600 = Y – 16000

Y = 1E980

Add image base 0101E980 (80 E9 01 01)

Code:

New entry point:

1BF50 – 13600 + 16000 = 1E950

Old entry point = jmp + Virtual address + 5 + R\_VA

01012475 = 0001E950 + image base + 14 + 5 + + R\_VA

R\_VA = FFFF 3B 0C

Payload

6A 00 68 70 E9 01 01 68 80 E9 01 01 6A 00 FF 15 A8 11 00 01 E9 0C 3B FF FF

4D 00 53 00 53 00 56 00 (MSSV)

32 00 30 00 35 00 32 00 31 00 33 00 31 00 37 00 2D 00 32 00 30 00 35 00 32 00 30 00 36 00 30 00 35 00 (20521317-20520605)

Graphical user interface, application

Description automatically generated