To Read the SB from Card:

* **Open From uncode32.dll**
* **Export**
* **InterpretCardContents**
* **F5 to view in C**

int \_\_userpurge **InterpretCardContents**@<eax>(const void \*a1@<eax>, int a2@<edx>, int a3@<ecx>, int ebx0@<ebx>, int a5, int a4)

{

v6 = a3;

qmemcpy(&v9, a1, 0x39u);

v7 = a3 - 1;

if ( v6 == 1 )

{

**result = sub\_412230(&v9, a4, (\_WORD \*)a5, ebx0); // 6. Doubble clck this Sub**

}

int \_\_usercall **sub\_412230**@<eax>(const void \*a1@<eax>, int a2@<edx>, \_WORD \*a3@<ecx>, int a4@<ebx>)

{

qmemcpy(&v45, a1, 0x39u); //7. Break Point here and read a1 (SB encoded and xored)//

v4 = (char \*)a1 + 57;

v48 = a3;

v49 = a2;

v36 = &savedregs;

v35 = &loc\_412781;

v34 = \_\_readfsdword(0);

\_\_writefsdword(0, (unsigned int)&v34);

System::\_\_linkproc\_\_ FillChar(a2, 304, 0);

System::\_\_linkproc\_\_ FillChar(&v44, 57, 0);

v5 = 33;

v6 = &v45;

v7 = &v44;

do

{

\*v7++ = \*v6++; //copy 186821 in 1867E8

--v5;

}

while ( v5 );

v8 = sub\_40ED20(&v44, 33, 1);

if ( v8 )

{

\_\_writefsdword(0, v34);

return v8;

}

v9 = sub\_4107B8(&v44); //v44 is v7 at 1867E8

**//Starting from here to read the two bytes**

\*v48 = v9;

**sub\_410DA0(&v44, &v42, v5, 0, (int)v4); // 9. double click this sub to read the two bytes PW**

v10 = v49;

int \_\_usercall sub\_410DA0@<eax>(const void \*a1@<eax>, \_DWORD \*a2@<edx>, int a3@<ebx>, void \*a4@<edi>, int a5@<esi>)

{

v22 = a3;

v21 = a5;

v20 = a4;

v26 = 0;

qmemcpy(a4, a1, 0x39u);

v27 = a2;

v19 = &savedregs;

v18 = &loc\_80B0EDC;

v17 = \_\_readfsdword(0);

\_\_writefsdword(0, (unsigned int)&v17);

**v5 = sub\_80AEDA4(6); //0x98 PASSWORD BYTE0**

**v6 = sub\_80AEDA4(6); //0x26 SCAMBLED PASSWORD BYTE0**

**v7 = sub\_80AEDA4(6); //0x73 SCAMBLED PASSWORD BYTE1**

**v8 = v6 \* sub\_80AED88(2) + v5; //0x98**

**v9 = sub\_80AED88(9); // 0x200**

**Sysutils::IntToStr(v7 \* v9 + v8);**

**System::\_\_linkproc\_\_ LStrSetLength(&v26, 8);// break here and read v8**

v10 = 1;

v11 = &v23;

**//BREAKING HERE IN V8 THE TWO BYTE 0xE698 INDON**

**//BREAKING HERE IN V8 THE TWO BYTE 0XBD7E JAUX**

**//BREAKING HERE IN V8 THE TWO BYTE 0XAF0C CREIL**

**//BREAKING HERE IN V8 THE TWO BYTE 0XD741 SDP**

**//BREAKING HERE IN V8 THE TWO BYTE 0XB0AD VTR**

**//BREAKING HERE IN V8 THE TWO BYTE 0XC2A5 NZZ**

**BZR**

**0xB0E8**

**STN**

**0xB127**

**LYN**

**0xD70D**

To write the SB to Card:

* Open Keycode32.dll
* Export
* VCKeyCode
* F5 to see in C
* Open First case

int \_\_stdcall **VCkeycode**(int a1, int a2, int a3)

{

int result; // eax@4

signed int v4; // ecx@7

bool v5; // zf@7

char v6; // [sp+0h] [bp-148h]@6

char v7[57]; // [sp+19h] [bp-12Fh]@8

\_\_int16 v8; // [sp+52h] [bp-F6h]@7

switch ( a2 )

{

**case 1:**

**result = sub\_A0D129B(a1, a3, 0); //6. Open this sub**

int \_\_cdecl **sub\_A0D129B(**int a1, int a2, int a3)

{

int result; // eax@1

CHAR OutputString; // [sp+4h] [bp-100h]@2

result = 0;

if ( \*(\_WORD \*)a2 == 328 )

{

switch ( a1 )

{

case 1:

case 2:

result = sub\_A0D2221(a1, a2, a3);

break;

case 3:

case 10:

case 11:

**result = sub\_A0D184C(a1, a2); //8. For FSK open case 3**

break;

case 4:

**result = sub\_A0D1B64(1, a2); //7. For PK open case 4**

9. For both PK and FSK point on the first memory to edit the buffer with the two Bytes

For PK:

v42 = 1;

**sub\_A0D2478(&v11, a2, 328); // 10. Break point her and read the buffer in a2**

v2 = 0;

0019C09B 00 00 00 00 48 01 00 00 00 00 **98 E6** 01 00 01 86

0019C0AB 57 2F 5F 38 57 2F 5F E0 52 31 5F B6 00 00 00 00

11. Change only these 2 bytes with the 2 pw bytes inverted:

**// TWO BYTE 0xE698 INDON**

**// TWO BYTE 0XBD7E JAUX Change 98 E6 with 7E BG**

**// 0XAF0C CREIL Change 98 E6 with 0C AF**

**// 0XD741 SDP Change 98 E6**

**// 0XB0AD VTR Change 98 E6 TO BE AD B0**

**// 0XC2A5 NZZ Change 98 E6 TO BE A5 C2**

**// 0XB0E8 BZR Change B0E8 TO BE E8 B0**

**// 0XB127 BZR Change B0E8 TO BE 0x27B1**

**//0xD70D LYN change to be 0x0DD7**

**Edit buffer G , apply, run and insert the card when prompted.**