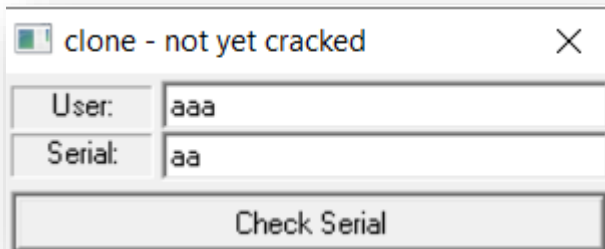


LẬP TRÌNH HỆ THỐNG– LỚP NT209.L21.ANTN




RE CHALLENGES: CLONE

Giảng viên hướng dẫn	Phạm Văn Hậu		ĐIỂM
Sinh viên thực hiện 1	Trần Đức Lương	19521815	

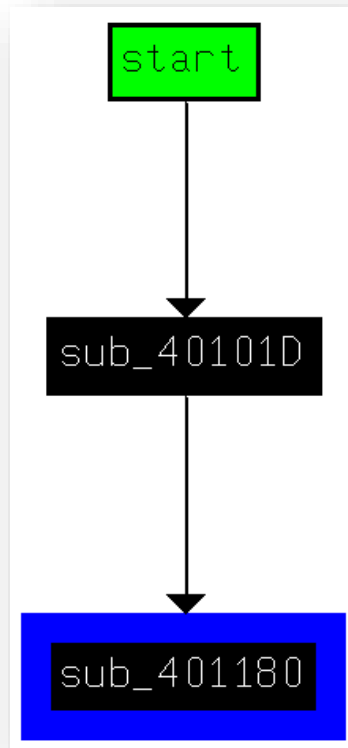
Thử chạy chương trình cho ra một giao diện đăng nhập với user và serial. Thử test như hình dưới thì thấy chương trình không thông báo gì, tức là đã không thành công.



Mở chương trình bằng IDA Pro, dùng strings thì thấy đây là những dòng thông báo thành công, tức là khi mình nhập đúng thì sẽ hiện ra những dòng này. Ý tưởng của bài có lẽ sẽ nhập user và serial sẽ phụ thuộc vào giá trị của user đó.

	.data:00403019	00000025	C	Well done! Now make good tutorial :)
	.data:0040303E	00000012	C	clone - defeated!
	.data:00403050	00000007	C	Bravo!

Đây là sơ đồ thực thi của chương trình với hàm start bắt đầu và gọi hàm sub_40101D().



Thực hiện quá trình xem mã giả của hàm sub_40101D() thì thấy ngay đầu hàm chương trình đã tiếp tục gọi hàm sub_401180().

```
u6.cbSize = 48;  
u6.style = 3;  
u6.lpfnWndProc = sub_401180;  
u6.cbClsExtra = 0;  
u6.cbWndExtra = 30;  
u6.hInstance = a1;  
u6.hbrBackground = (HBRUSH)16;
```

Trong hàm sub_401180() xuất hiện dòng if bên dưới. Sau khi debug thì thấy byte_40307C chính là biến lưu user và String là biến lưu serial. Cụ thể user phải có số kí tự ít nhất là 5 và serial có đúng 8 kí tự.

```
if ( lParam
    && wParam == 103
    && GetDlgItemTextA(hWnd, 102, String, 25) == 8
    && GetDlgItemTextA(hWnd, 101, byte_40307C, 30) >= 5 )
```

Block code dưới nằm trong hàm `sub_401180()` nhằm xử lý thông tin từ user. Cái mình cần quan tâm ở đây là giá trị của biến `dword_4030C8` sau khi chạy xong block này vì `dword_4030C8` sẽ được dùng cho quá trình tiếp theo.

```

u4 = 2byte_40307C[4];
u5 = 0;
do
    u5 += *u4++;
while ( *u4 );
LOBYTE(u6) = u5;
HIBYTE(u6) = u5;
u7 = _byteswap_ulong(u6);
LOBYTE(u7) = u5;
BYTE1(u7) = u5;
u8 = _byteswap_ulong(_byteswap_ulong(_byteswap_ulong(*(_DWORD *)byte_40307C ^ u7) + 56470918) + 559038242);
LOBYTE(u8) = u8 + 1;
++BYTE1(u8);
u9 = _byteswap_ulong(u8);
LOBYTE(u9) = u9 - 1;
--BYTE1(u9);
u10 = _byteswap_ulong(*(_DWORD *)byte_40307C + _byteswap_ulong(_byteswap_ulong(_byteswap_ulong(_byteswap_ulong(_byteswap_ulong(
LOWORD(u10) = u10 + 1;
u11 = _byteswap_ulong(u10);
LOWORD(u11) = u11 + 1;
dword_4030C8 = _byteswap_ulong(u11);

```

Sau khi debug với user = “11111” thì nhận được dword_4030C8 = 0x514081B1 (Little Endian)

```
.data:004030C8 dword_4030C8 dd 514081B1h
.data:004030C8
```

Bên dưới đây là block xử lí thông tin từ serial, cụ thể hàm này chỉ rõ ra các ký tự của serial chỉ nằm trong dãy các kí tự là ('0','1','2','3','4','5','6','7','8','9','A','B','C','D','E','F'). Và hơn nữa byte_4030B8 bây giờ sẽ là một mảng lưu mã hex thật của các ký tự trong khoảng trên. VD chuỗi là "ABC12345" thì byte_4030B8 = {0xA,0xB,0xC,0x1,0x2,0x3,0x4,0x5}

```

v12 = 0;
v13 = (unsigned __int8 *)String;
while ( 1 )
{
    v14 = *v13;
    if ( !*v13 )
        break;
    if ( v14 < 0x30u )
        return 0;
    if ( v14 > 0x39u )
    {
        if ( v14 < 0x41u || v14 > 0x46u )
            return 0;
        byte_4030B8[v12] = v14 - 55;
        ++v13;
        ++v12;
    }
    else
    {
        byte_4030B8[v12] = v14 - 48;
        ++v13;
        ++v12;
    }
}

```

Dòng if này chính là điều kiện chúng ta cần check, nếu đúng thì chương trình sẽ báo thành công.

```

if ( dword_4030C8 == _byteswap_ulong((unsigned __int8)(((byte_4030B8[7] + 16 * byte_4030B8[6]) ^ 0xCD) - 17) + (((unsigned __int8)(((byte_4030B8
{
    MessageBox(0, Text, Caption, 0x40u);
    SetWindowTextA(hWnd, aCloneDefeated);
}

```

Đại loại của dòng if trên sẽ là so sánh xem giá trị tính toán dựa trên byte_4030B8 có bằng với dword_4030C8 không. Như phân tích trên dùng với user = “11111” nên ta có: dword_4030C8 = 0x514081B1 (Little Endian).

Cụ thể khi đó: (s chính là byte_4030B8)

$s[i]$ thuộc

$\{0x0, 0x1, 0x2, 0x3, 0x4, 0x5, 0x6, 0x7, 0x8, 0x9, 0xA, 0xB, 0xC, 0xD, 0xE, 0xF\}$

- $(s[1] + s[0] \ll 4) \wedge 0x12 + 0x34 = 0xB1 \Rightarrow (s[1] + s[0] \ll 4) = 0x6F \Rightarrow s[0] == 0x6 \text{ ('6')}, s[1] == 0xF \text{ ('F')}$
- $(s[3] + s[2] \ll 4) \wedge 0x56 + 0x78 = 0x81 \Rightarrow (s[3] + s[2] \ll 4) = 0x5F \Rightarrow s[2] == 0x5 \text{ ('5')}, s[3] == 0xF \text{ ('F')}$
- $(s[5] + s[4] \ll 4) \wedge 0x90 + 0xAB = 0x40 \Rightarrow (s[5] + s[4] \ll 4) = 0x05 \Rightarrow s[4] == 0x0 \text{ ('0')}, s[5] == 0x5 \text{ ('5')}$
- $(s[7] + s[6] \ll 4) \wedge 0xCD + 0xEF = 0x51 \Rightarrow (s[7] + s[6] \ll 4) = 0xAF \Rightarrow s[6] == 0xA \text{ ('A')}, s[7] == 0xF \text{ ('F')}$

Suy ra serial cần tìm để dòng if đó đúng là : “6F5F05AF”

Thực hiện đăng nhập với kết quả trên ta nhận được thông báo thành công của chương trình.

