链滴

C++ 的一些奇技淫巧

作者：Private

原文链接：https://ld246.com/article/1553433239250

来源网站：链滴

获取类的构造函数地址

C++标准明确规定了，不能取构造函数的地址

虽然正常方法不能获取构造函数的地址，但是我们可以另辟蹊径，借助**汇编**来达到我们的目的

1. 显式调用构造函数，但是不让构造函数执行(通过 **goto**语句跳过构造函数)
2. 通过反汇编解析调用构造函数的C++代码所生成的机器代码得到构造函数地址

```
template<class T>
void * GetConstructorAddr()
{
    goto Start;
Call_Constructor:
    //这行代码不会执行，代码的目的是为了让编译器生成调用构造函数相应的汇编代码
    //通过解析汇编代码，就可以得到构造函数的地址
    T();
Start:
    //通过汇编得到 T() 这行代码的地址
    char * p = nullptr;
    __asm
    {
        MOV EAX, OFFSET Call_Constructor
        MOV DWORD PTR[p], EAX
    }
    p += 6;
    int offset = *(int *)(p + 1);
    void * ret = p + 5 + offset;//p+5 = EIP

    return ret;
}
```

上面代码在 vs2015 环境下验证没问题，其他环境不保证，这里只是提供一个思路

To be continued ...