proc, void* pThis) { m_mov = 0xB9. m_this = PtrToUlong(pThis). m_jmp = 0xe9. m_relproc = DWORD((INT_PTR)proc - ((INT_PTR)this sizeof(MemFunToStdCallThunk))). ::FlushInstructionCache(::GetCurrentProcess(), this, sizeof(MemFunToStdCallThunk)). return TRUE. } void* GetCodeAddress() { return this. } }. #pragma pack(pop) 这个结构相当于两条汇编语句： mov ecx, pThis jmp [偏移地址] 使用： class CTestClass { private: int m_nBase. MemFunToStdCallThunk m_thunk. void memFun(int m, int n) { int nSun = m_nBase m n. CString str. str.Format(_T("%d"), nSun). AtlMessageBox(NULL, _U_STRINGorID(str)). } public: CTestClass() { m_nBase = 10. } void Test() { //UnionCastType:利用联合将函数指针转换成DWORD_PTR m_thunk.Init(UnionCastType 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com