Detours

김영철

2015. 11. 17.

Detours

- DetourAttach() function

```
LONG WINAPI DetourAttach(PVOID *ppPointer,
                         PVOID pDetour);
```

first parameter :: detour 될 함수의 포인터의 포인터
second parameter :: detour 할 함수의 포인터

Hooking by Detours

- 후킹 과정

  DetourTransactionBegin()

  ➔ 후킹 또는 후킹해제를 위한 준비

  DetourUpdateThread(GetCurrentThread())

  ➔ 현재 프로세스의 Thread handle

  DetourAttach(PVOID *ppPointer, PVOID pDetour)

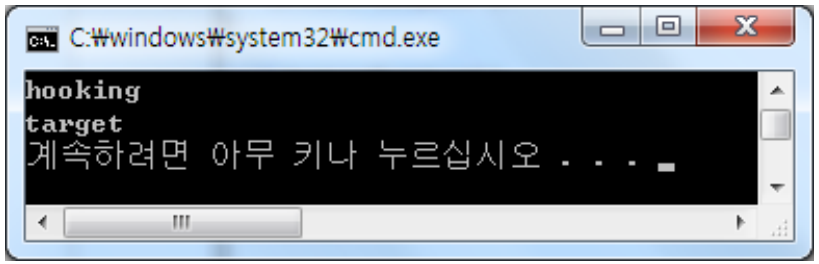
  ➔ 후킹 할 함수 조작

  DetourTransactionCommit()

  ➔ 후킹 실행

Hooking by Detours

```
void targetFunction( )
{
    printf("target₩n");
}

void hookingFunction( )
{
    printf("hooking₩n");
}

int main( )
{
    void (*target)( )=targetFunction;
    DetourTransactionBegin( );
    DetourUpdateThread(GetCurrentThread( ));
    DetourAttach((PVOID*)&target, hookingFunction);
    DetourTransactionCommit( );
    targetFunction( );

    DetourTransactionBegin( );
    DetourUpdateThread(GetCurrentThread( ));
    DetourDetach((PVOID*)&target, hookingFunction);
    DetourTransactionCommit( );
    targetFunction( );

    return 0;
}
```

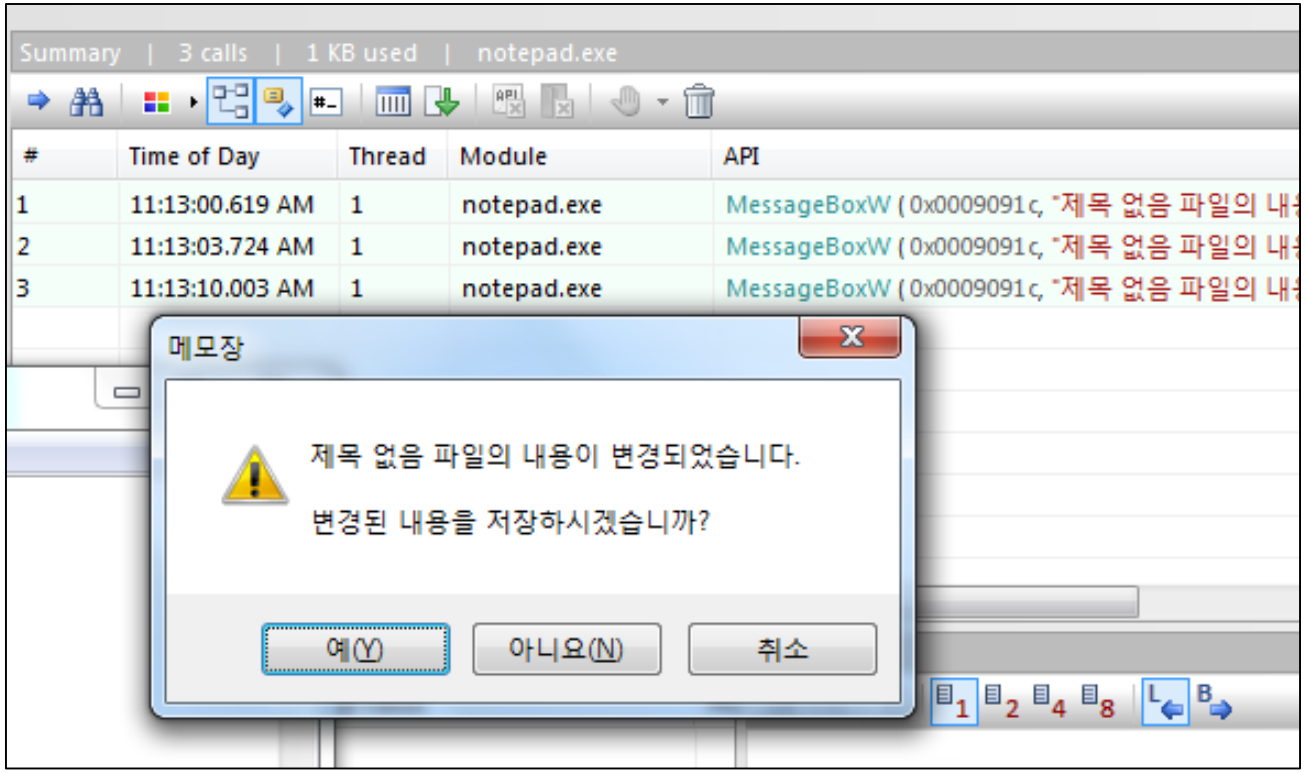


API hooking

- 시나리오
  1. API Monitor를 이용, 호출 함수 모니터링
  2. 타겟 함수 선택
  3. 변조 함수 구현
  4. DLL Attach될 경우 detour를 이용하여 후킹

API hooking

- API Monitor의 함수 호출 모니터링



API hooking

- 타겟 함수 설정, 변조 함수 구현

```
static int (WINAPI *target)(HWND, LPCWSTR, LPCWSTR, UINT) = MessageBoxW;

int WINAPI fakeMessageBox(HWND hWnd, LPCWSTR lpText, LPCWSTR lpCaption, UINT uiType)
{
    return target(hWnd, L"Hooked", L"Fake", uiType);
}
```

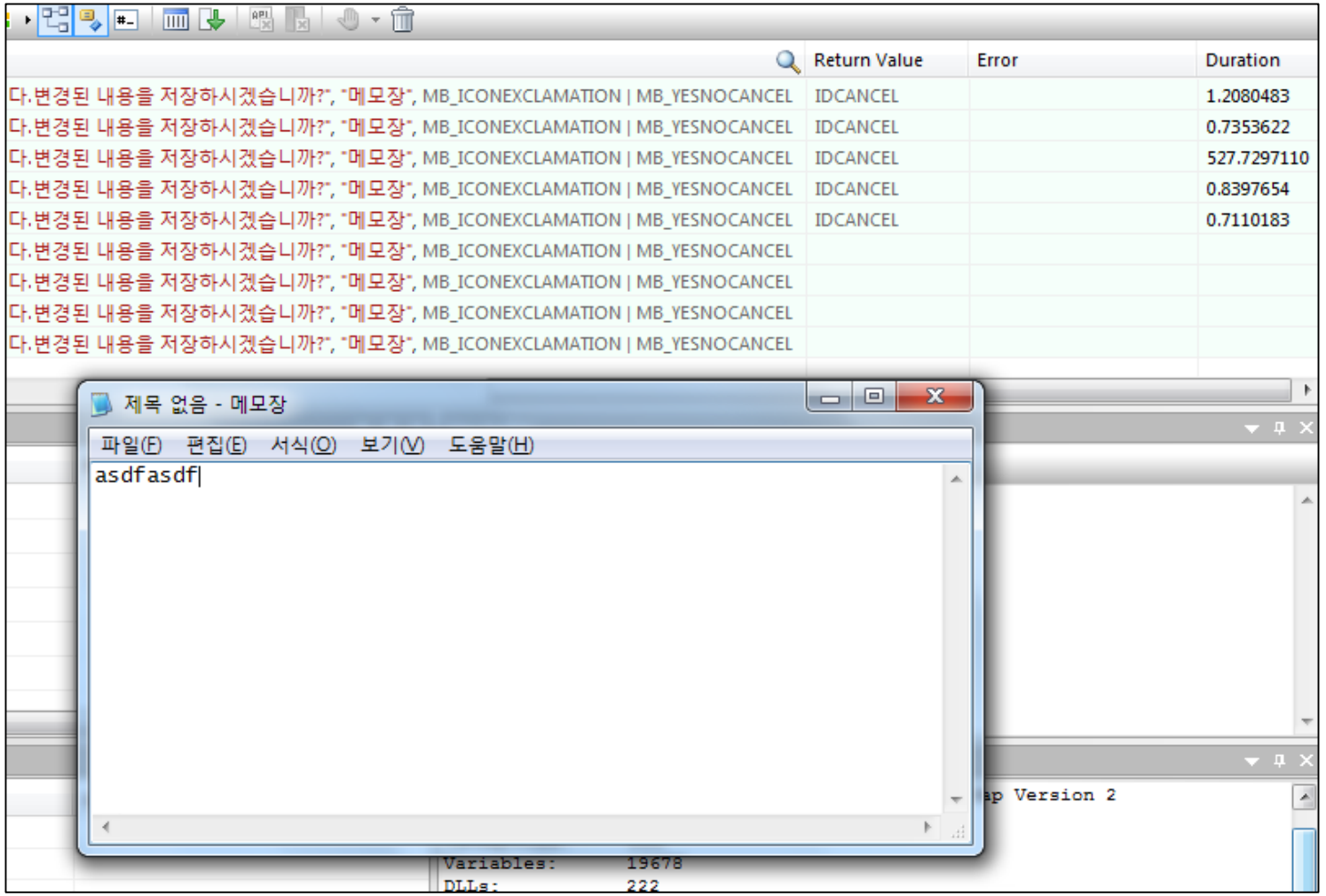
API hooking

- DLL_Main 구현

```
long error;
int WINAPI DllMain(HINSTANCE hinstDLL, DWORD fdwReason, LPVOID lpvReserved)
{
    switch(fdwReason)
    {
    case DLL_PROCESS_ATTACH:
        DetourRestoreAfterWith();

        DetourTransactionBegin();
        DetourUpdateThread(GetCurrentThread());

        DetourAttach( &(PVOID&)target, fakeMessageBox);

        error = DetourTransactionCommit();
        if(error == NO_ERROR)
            OutputDebugString("Injection Success!!!");
        break;
    }

    return 0;
}
```

API hooking

- 실패..



API hooking

- 실패..