

# ONLINE GAME HACKING



강민수(강명석)  
Email : admin@hack.kr

51 ALIVE

[808m] CucksonParade M16A4

[836m] TCUCheech15 SCAR-L

[966m] George-Green Barrett

[1521m] yekonyx

[1630m] Pengu1530x SCAR

[1661m] TripleTact

[1800m] zhenNipp

[1800m] Maimi Lightning

[1800m] Winchester

Piguin killed Tutetillo11 with M16A4 - 52 left

Liquifiedsnails died from falling - 51 left

10 | 30

AUTO

CS L4 D0 D1 D2

L5

L6

L7

# CULTURE

전체글보기

베스트게시글

이미지모아보기

동영상모아보기

카페테그보기

매니저

데블군

since 2006.06.03.

카페소개

앞새2단계

15,876

게시판 구독수

0회

우리카페앱 수

0회

초대

카페 채팅

카페 가입하기

전체글보기 (37,695)

검색

동영상형

앨범형

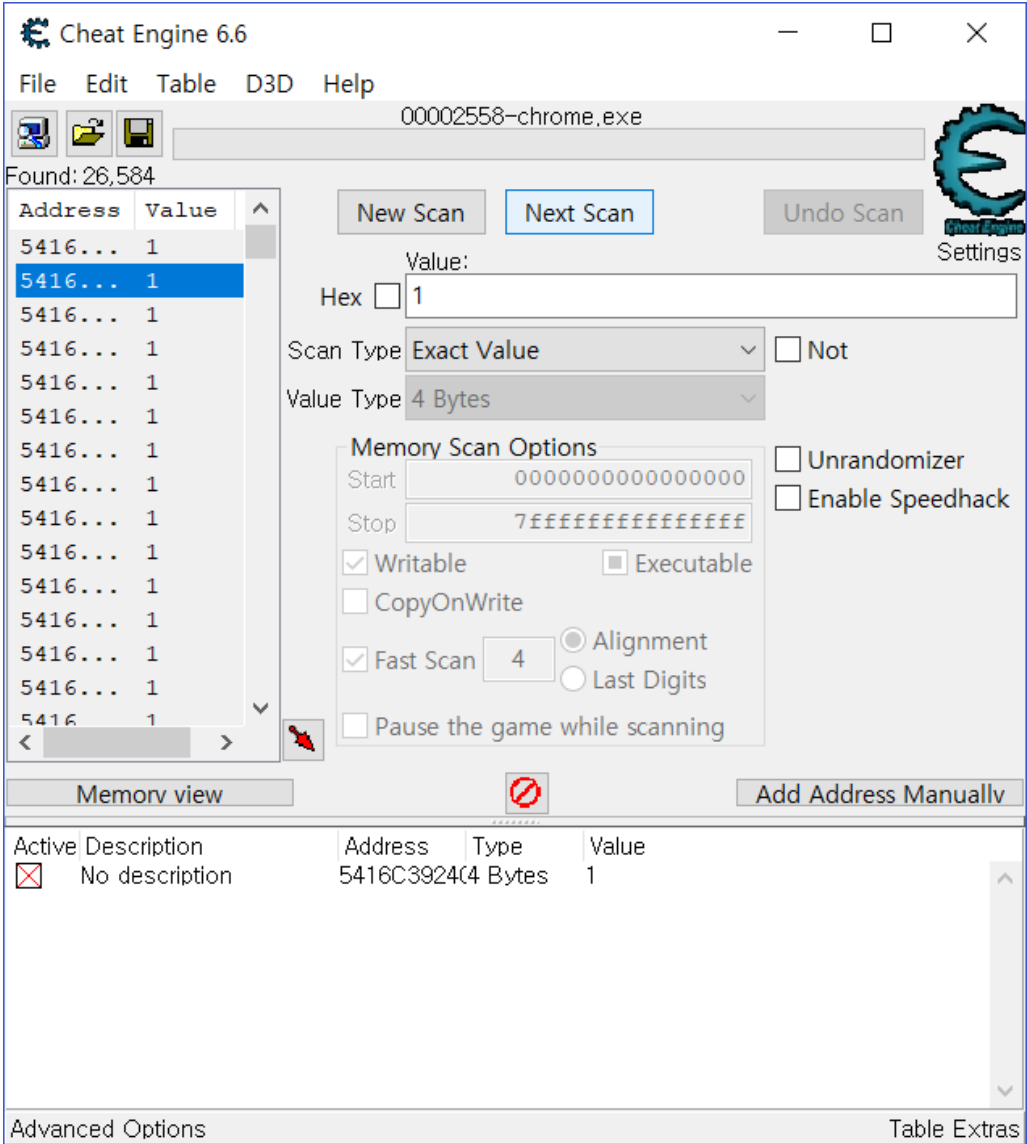
게시판형

공지 숨기기

15개씩 보기

제목	작성자	작성일	조회	좋아요
비 매테오 버그 쿠와와와 의 강좌 (스샷첨부)  [18] <a href="#">답글 1개</a> ▼	쿠와와와	2007.02.18,	447	0
37779 벽짬해주시분	wodnd5398	2007.02.18,	5	0
37777 ※ 기억버그 (기안다는 버그) 쿠와와와 의 강의 ※  [17]	쿠와와와	2007.02.18,	398	0
37776 다크어썸로 전직해야되는데..	tls21136	2007.02.18,	8	0
37773 하층,상층 버그 돌립니다. [15]	휘프노스	2007.02.17,	125	0
37772 코스튬 버그 쓰면 아템이 자꾸 사라짐	secretit	2007.02.17,	35	0

# CHEAT ENGINE



# CHEAT ENGINE

```
DWORD dwOld;
VirtualProtect((void*)0x08048fb7, 1, PAGE_EXECUTE | PAGE_GUARD, &dwOld); // This sets the protection for
                                                                    // Which is going to cause an e

AddVectoredExceptionHandler(true, (PVECTORED_EXCEPTION_HANDLER)UnhandledExceptionFilter); // Registers ou

unsigned long UnhandledExceptionFilter(EXCEPTION_POINTERS *pExceptionInfo)
{
    if (pExceptionInfo->ExceptionRecord->ExceptionCode == STATUS_GUARD_PAGE_VIOLATION) // This is going t
    {
        if (pExceptionInfo->ContextRecord->Eip == 0x08048fb7) // Here we check to see if the instruction
        {
            dwJmpBack = (DWORD*)(pExceptionInfo->ContextRecord->Esp + 0); // Find the return address for
            dwJmpBack = (DWORD)pExceptionInfo->ContextRecord->Eip + 5; // or just skip X number of bytes.
            pExceptionInfo->ContextRecord->Eip = (DWORD)hkFunction; // Point EIP to hook handle.
        }

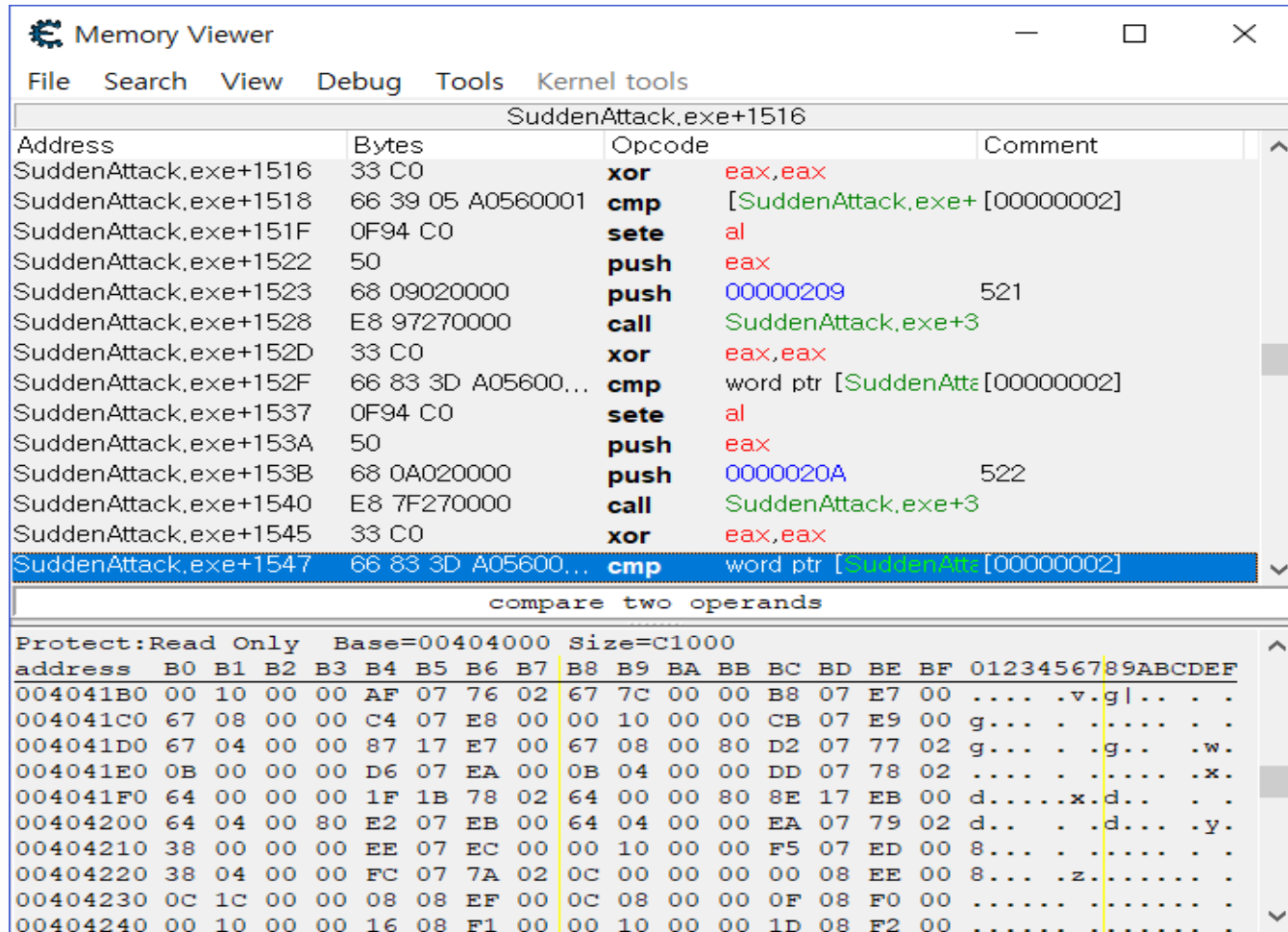
        pExceptionInfo->ContextRecord->EFlags |= 0x100; //Set single step flag, causing only one line of

        return EXCEPTION_CONTINUE_EXECUTION; // When we return to the page, it will no longer be PAGE_GUAR
    }
}
```

# REVERSING == HACK

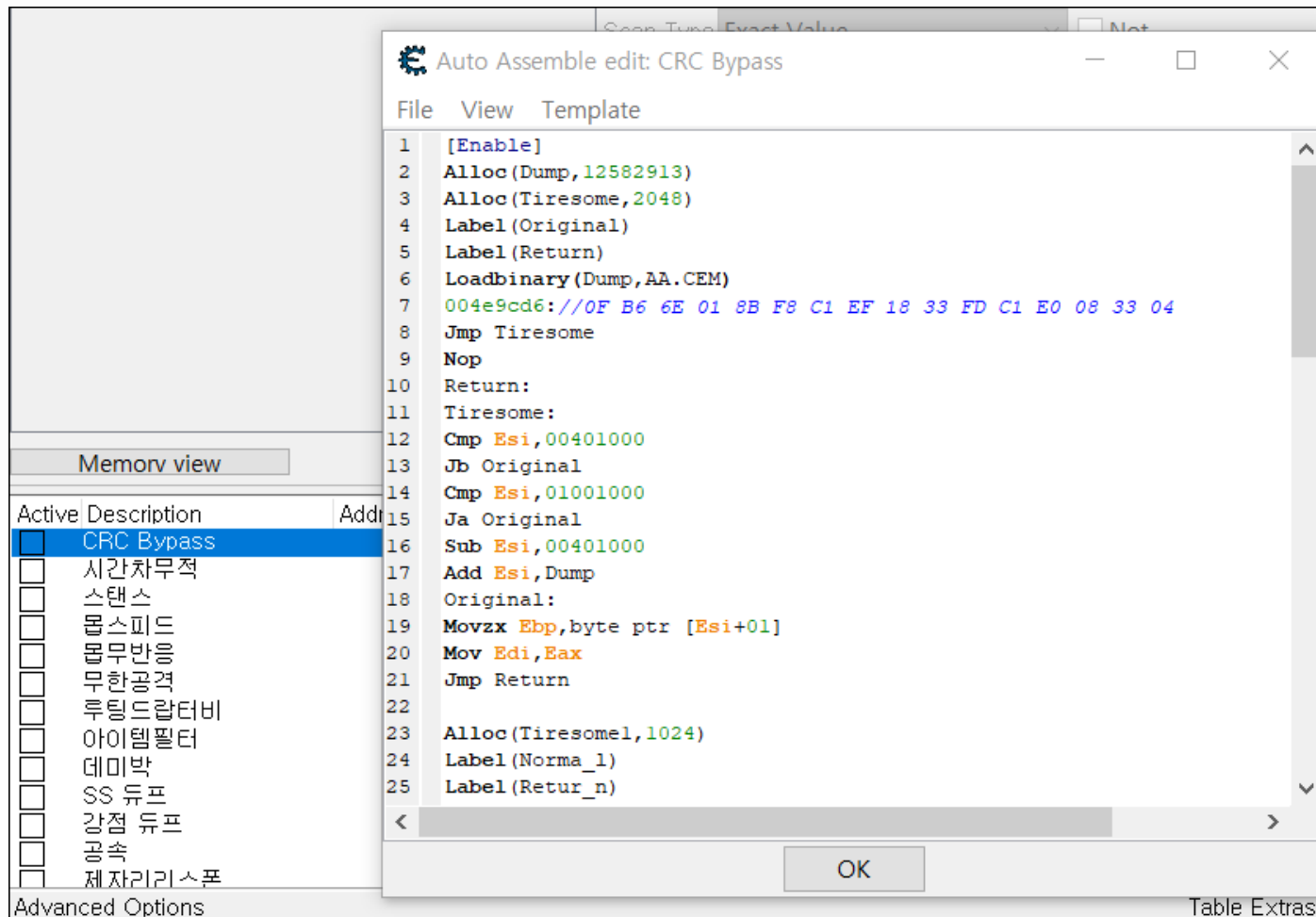


# CRC





# CRC - BYPASS





# CRC - BYPASS



# DLL INJECTION

```
do
{
    dwProcess = (DWORD)GetModuleHandleA("Process_name");
    Sleep(40);
} while (!dwProcess);

Sleep(500);
printf("PID: %x\\n", dwProcess);
}

BOOL APIENTRY DllMain(HMODULE hModul, DWORD ul_reason_for_ca, LPVOID lpReserve)
{
    switch (ul_reason_for_ca)
    {
    case DLL_PROCESS_ATTACH:
        DisableThreadLibraryCalls(hModul);
        AllocConsole();
        freopen( "CON", "w", stdout );
        CreateThread(NULL, NULL, (LPTHREAD_START_ROUTINE)Module, NULL, NULL, NULL);
        MessageBoxA(NULL, "Start!", "By Empier", MB_OK);
    case DLL_THREAD_ATTACH:
    case DLL_THREAD_DETACH:
    case DLL_PROCESS_DETACH:
        break;
    }
}
```

# HOOKING

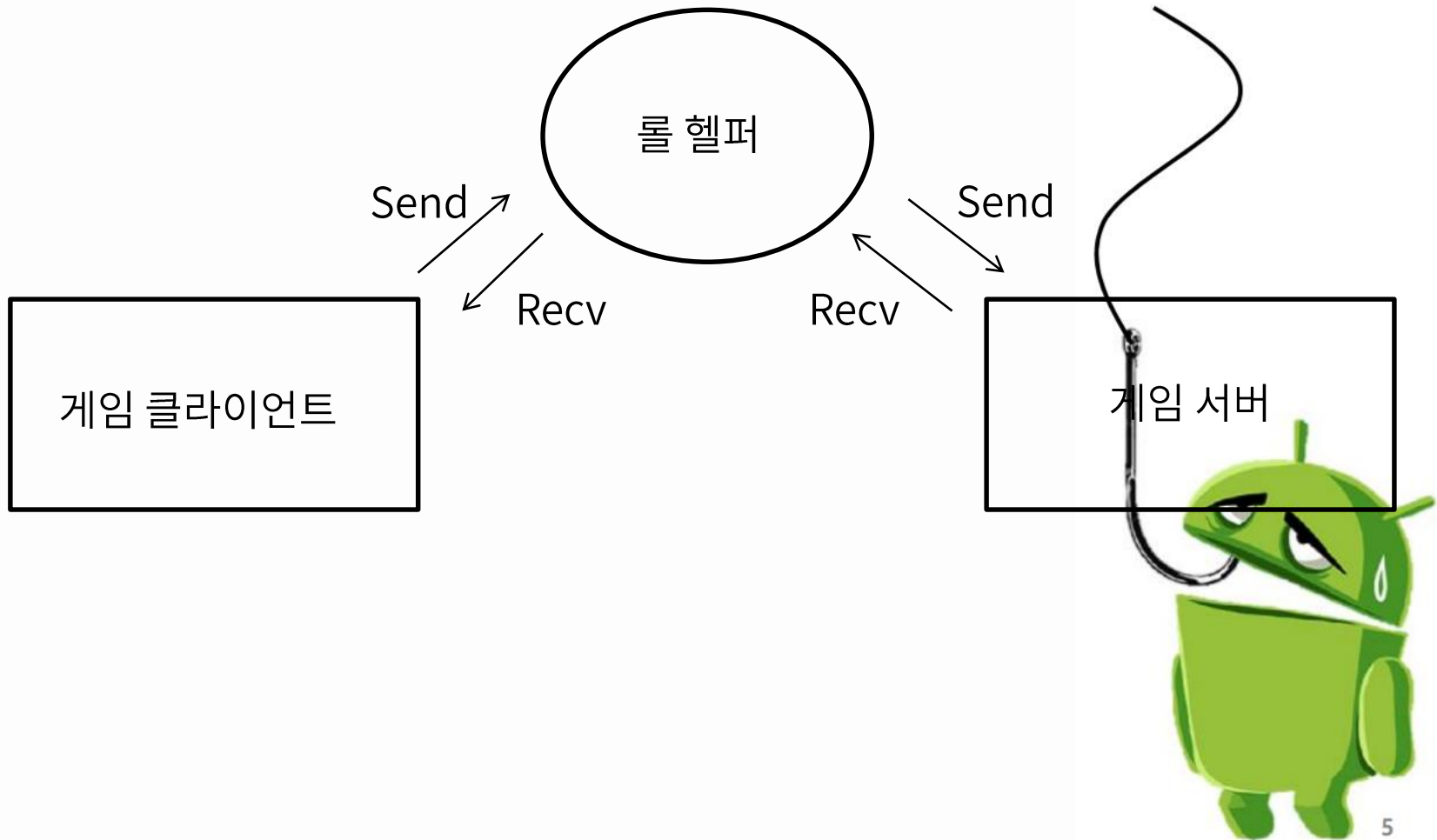


# HOOKING

- 1) Connect 함수를 후킹
- 2) 내 프로그램의 소켓으로 연결
- 3) 내 소켓에서 패킷을 복호화하고 원하는 대로 패킷을 변조
- 4) 다시 암호화 하여 원래 목적지로 전송



# HOOKING



# SCRIPT

```
return 0;
```

```
//printf("HANDLE: %x\n",L);
luaL_openlibs(L);
lua_register(L, "showtext", lua_showtext);
lua_register(L, "say", lua_say);
lua_register(L, "do_command", lua_do_command);
lua_register(L, "sleep", lua_sleep);
lua_register(L, "rand", lua_rand);
lua_register(L, "keypress", lua_keypress);
lua_register(L, "keyup", lua_keyup);
lua_register(L, "keydown", lua_keydown);
```

```
int lua_sleep(lua_State* L)
{
    unsigned int a = 0;

    a = (int)luaL_checkinteger(L, 1);
    sleep(a);
    return 0;
}
```

# DEMO

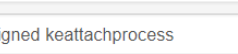




# DRIVER

```
v5 = a4;
v6 = a3;
Object = 0i64;
v7 = 0xC0000001;
if ( PsLookupProcessByProcessId(a1, &Object) >= 0 )
{
    KeAttachProcess(Object);
    if ( sub_13604(v6) && sub_13604(v5 + v6 - 1) )
    {
        v9 = dword_24304;
        if ( dword_24304 )
        {
            _disable();
            sub_14A50();
            v9 = dword_24304;
        }
        for ( i = 0; i < (unsigned int)v5; ++i )
            *(_BYTE *)(i + v6) = *(_BYTE *)(i + a5); // WriteProcessMemory
        v7 = 0;
        if ( v9 )
        {
            LODWORD(v11) = sub_14AC8();
            v12 = v11;
            sub_14A8C();
            _enable();
            DbgPrint("lastError=%p\\n", v12);
            if ( v12 )
                v7 = 0xC0000001;
        }
    }
    KeDetachProcess();
    ObfDereferenceObject(Object);
    result = (v7 & 0x80000000) == 0;
}
```

# DRIVER



247 files found


File	Ratio	First sub.	Last sub. ▼	Times sub.	Sources	Size
<input type="checkbox"/> <div> 22b1df2a21ecdb6ac24bb3f5fb5718a16bf665f15dd71ca3b51fd4ff2ab68bb112888499a5f381ab9a0cf2ddfe8fbc </div> <div> <input type="button" value="peexe"/> <input type="button" value="assembly"/> <input type="button" value="overlay"/> <input type="button" value="signed"/> <input type="button" value="64bits"/> <input type="button" value="native"/> </div>	2 / 64	2018-07-02 16:53:17	2018-07-02 16:53:17	1	1	16.5 KB
<input type="checkbox"/> <div> f85de9cf0f1b0354903789f3d5dd2b8afaf53148a9e4f14235e1835a096cae3a7f476fba979f1df949e387faafd0fb8e </div> <div> <input type="button" value="peexe"/> <input type="button" value="assembly"/> <input type="button" value="overlay"/> <input type="button" value="revoked-cert"/> <input type="button" value="signed"/> <input type="button" value="64bits"/> <input type="button" value="native"/> </div>	3 / 63	2018-07-02 13:00:42	2018-07-02 13:00:42	1	1	12.8 KB
<input type="checkbox"/> <div> 85eb616ab4424ea27ea3dcd7df1a8b7a5ed8e533212927e2b1dfb03679c758fe71a3adbe7eb8aed5fe7c97f8451eb2c </div> <div> <input type="button" value="peexe"/> <input type="button" value="assembly"/> <input type="button" value="overlay"/> <input type="button" value="signed"/> <input type="button" value="64bits"/> <input type="button" value="native"/> </div>	5 / 64	2018-07-02 08:53:10	2018-07-02 08:53:10	1	1	16.6 KB
<input type="checkbox"/> <div> 50bf5b7626970f5213cacf595b1f442b7538665228e768c13c2feb2b0485b919f5bedb5bd7534608ca4958a8b0f82bcd </div> <div> <input type="button" value="peexe"/> <input type="button" value="assembly"/> <input type="button" value="overlay"/> <input type="button" value="revoked-cert"/> <input type="button" value="signed"/> <input type="button" value="64bits"/> <input type="button" value="native"/> </div>	33 / 63	2018-07-02 00:56:20	2018-07-02 00:56:20	1	1	113.8 KB
<input type="checkbox"/> <div> 4a7e5833d17765a12f53dc2371739dc9a463940b13e16157ce10db80e958d740548260a7b8654e024dc30bf8a7c5baa4 </div> <div> <input type="button" value="peexe"/> <input type="button" value="assembly"/> <input type="button" value="overlay"/> <input type="button" value="revoked-cert"/> <input type="button" value="signed"/> <input type="button" value="64bits"/> <input type="button" value="native"/> </div>	0 / 64	2010-02-11 15:38:47	2018-07-01 19:20:27	349	45	91.0 KB

# SECURITY



# MOBILE


[HOME](#) [FORUMS](#) [WHAT'S NEW](#) [VIP MODS](#) [SEARCH](#) [BUY VIP](#) [Log in](#) [Register](#)

 **Licensed** **Seven Knights (KR) / 세븐나이즈 5.1.71** NO PERMISSION TO DOWNLOAD

[TeamAR](#) · Oct 24, 2015 · [netmarble](#) [vip mod](#)

[Forums](#) > [VIP Mods](#) > [VIP](#) > **Korean Games**

[OVERVIEW](#) [UPDATES \(75\)](#) [REVIEWS \(13\)](#) [HISTORY](#)



**ALL NEW <세븐나이즈> 각성 업데이트!**

**Root Needed?:** No  
**License Needed?:** Yes

**Mod:**  
1.) x10 damage  
2.) x10 def

**Install Steps:**  
1.) Install and Enjoy.

**Playstore Link:** [세븐나이즈 for Kakao - Android Apps on Google Play](#)  
👍 MrMelendres11, Lazy662, uNams86 and 21 others

Author: [TeamAR](#)  
Downloads: 1,150  
First release: Oct 24, 2015  
Last update: Sunday at 10:39  
Rating: ★★★★★  
13 ratings

[Forums](#) > [VIP Mods](#) > [VIP](#) > **Korean Games**

끝으로..

# QnA