ON-LINE GAME HACKING

강민수(강명석) admin@hack.kr

HACKING

CodeEngn

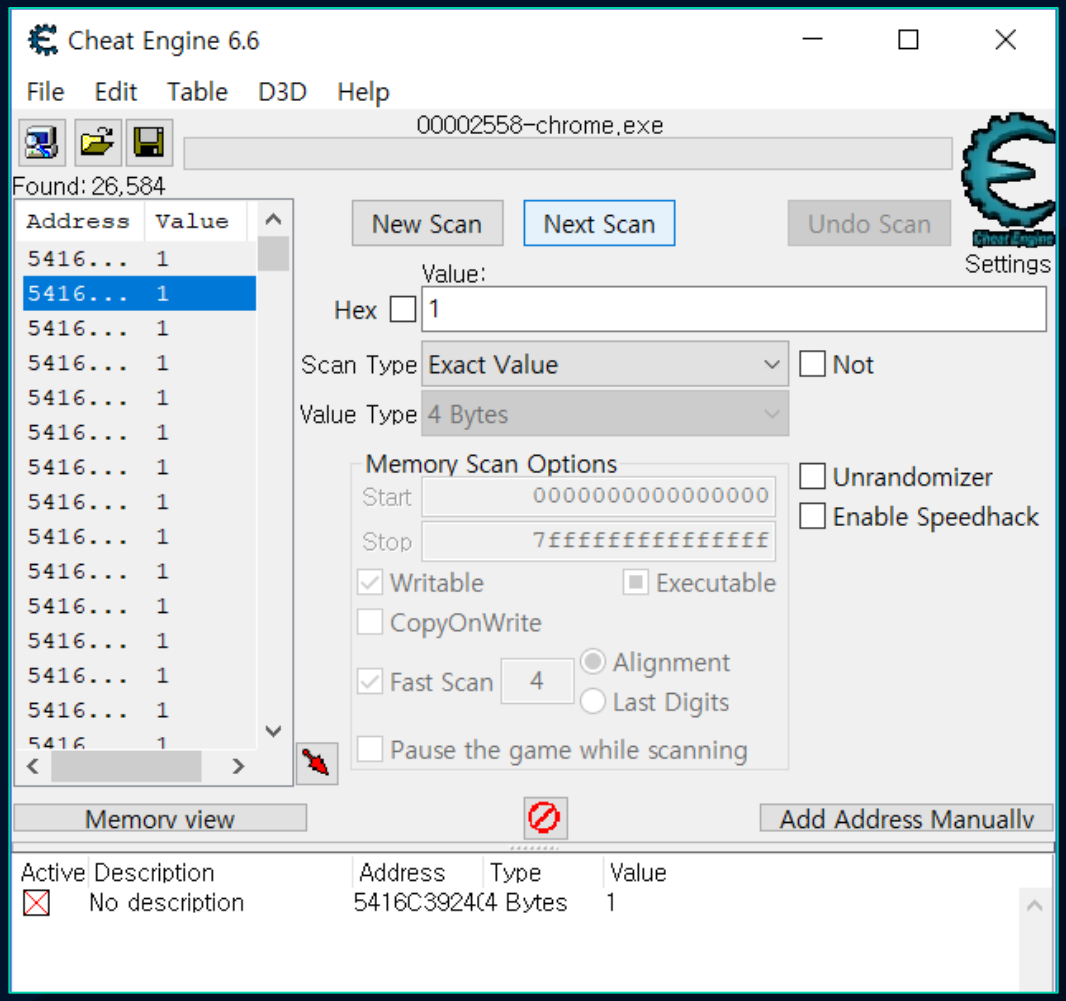
GAME HACK

HACKING

CULTURE

HACKING

CHEAT ENGINE



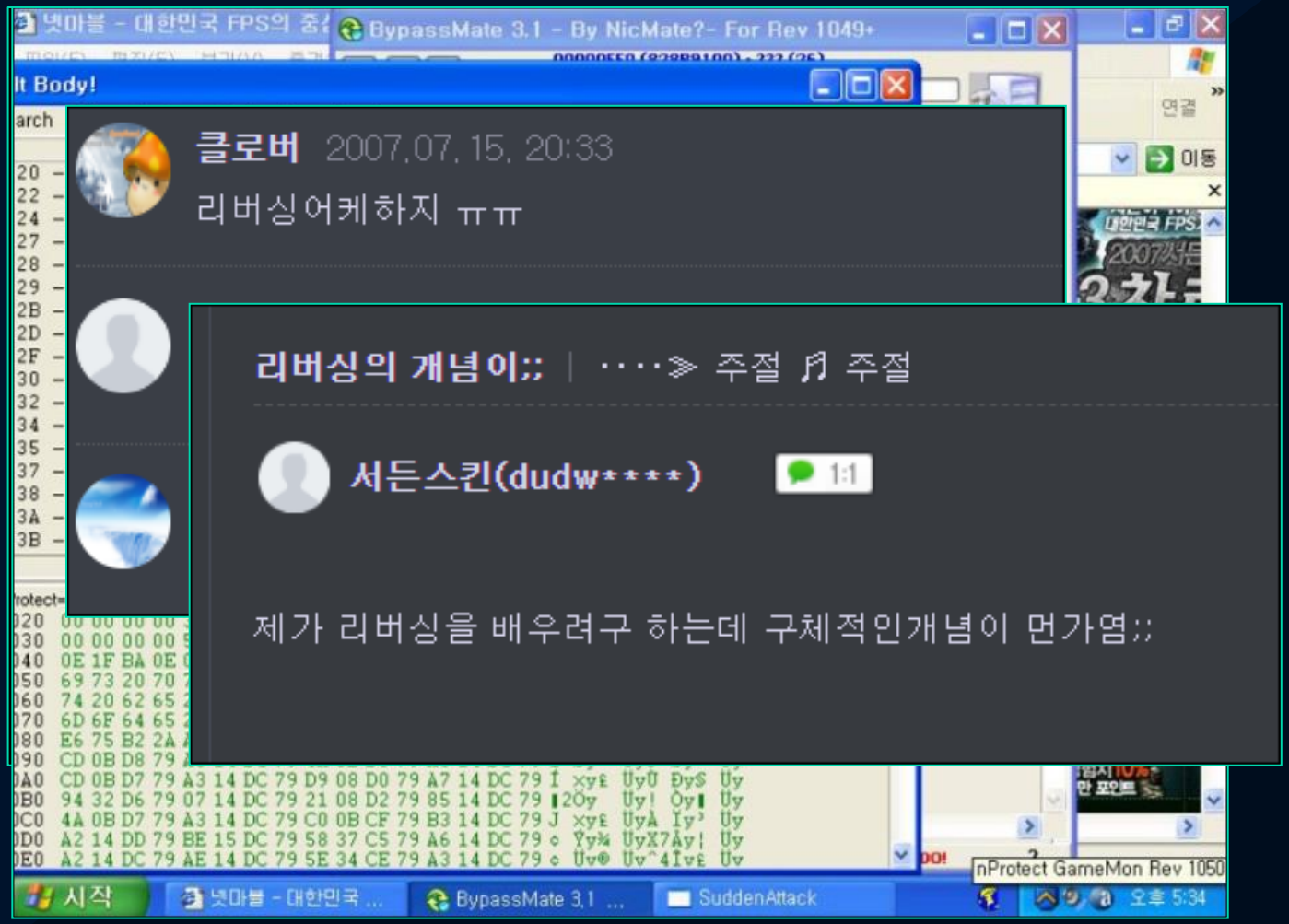
HACKING

CHEAT ENGINE

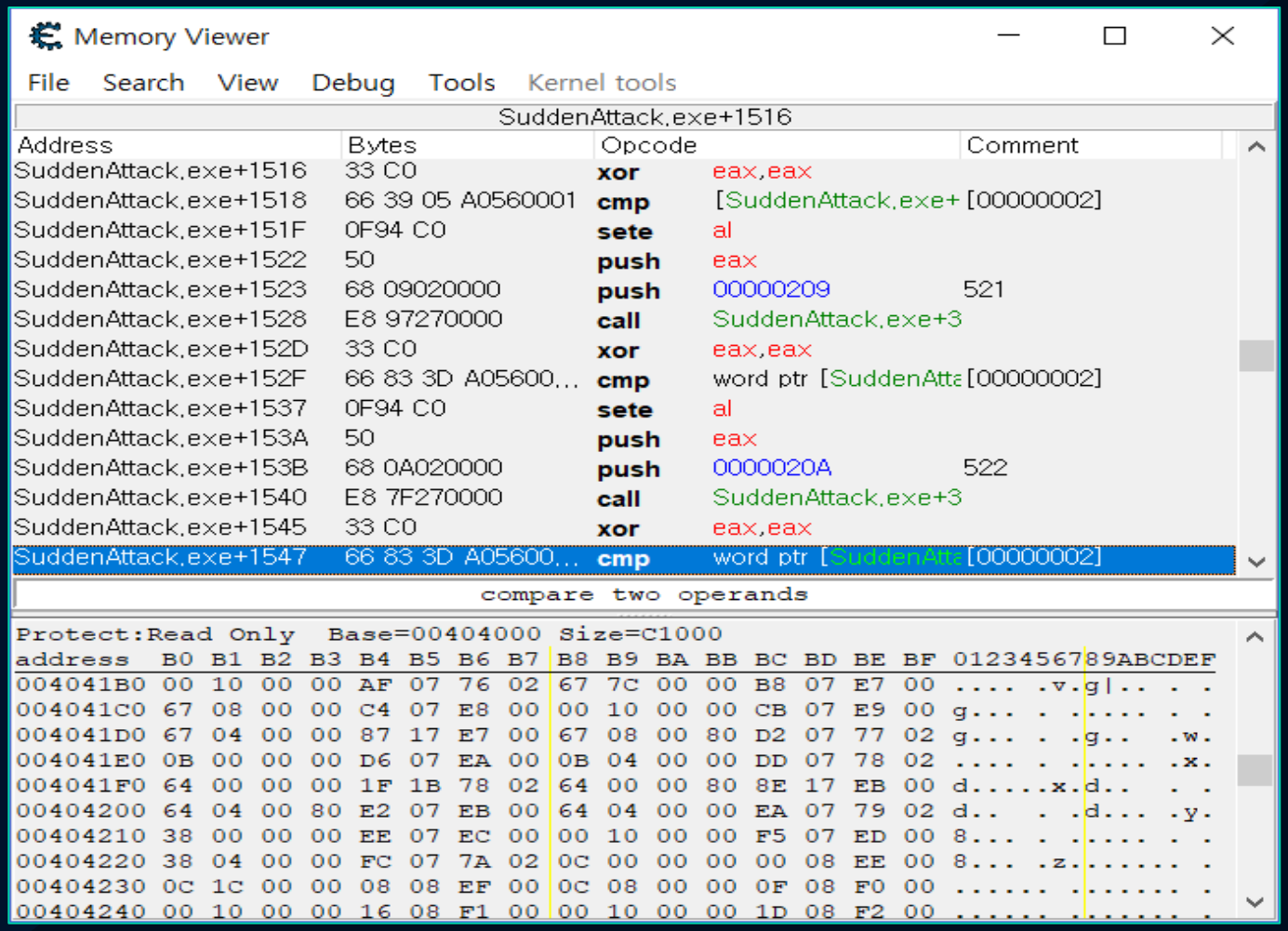
```
DWORD dwOld;
VirtualProtect((void*)0x08048fb7, 1, PAGE_EXECUTE | PAGE_GUARD, &dwOld); // This sets the protection for
                                                                         // Which is going to cause an e

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_GUA
    }
```

HACKING

REVERSING = HACK



CRC

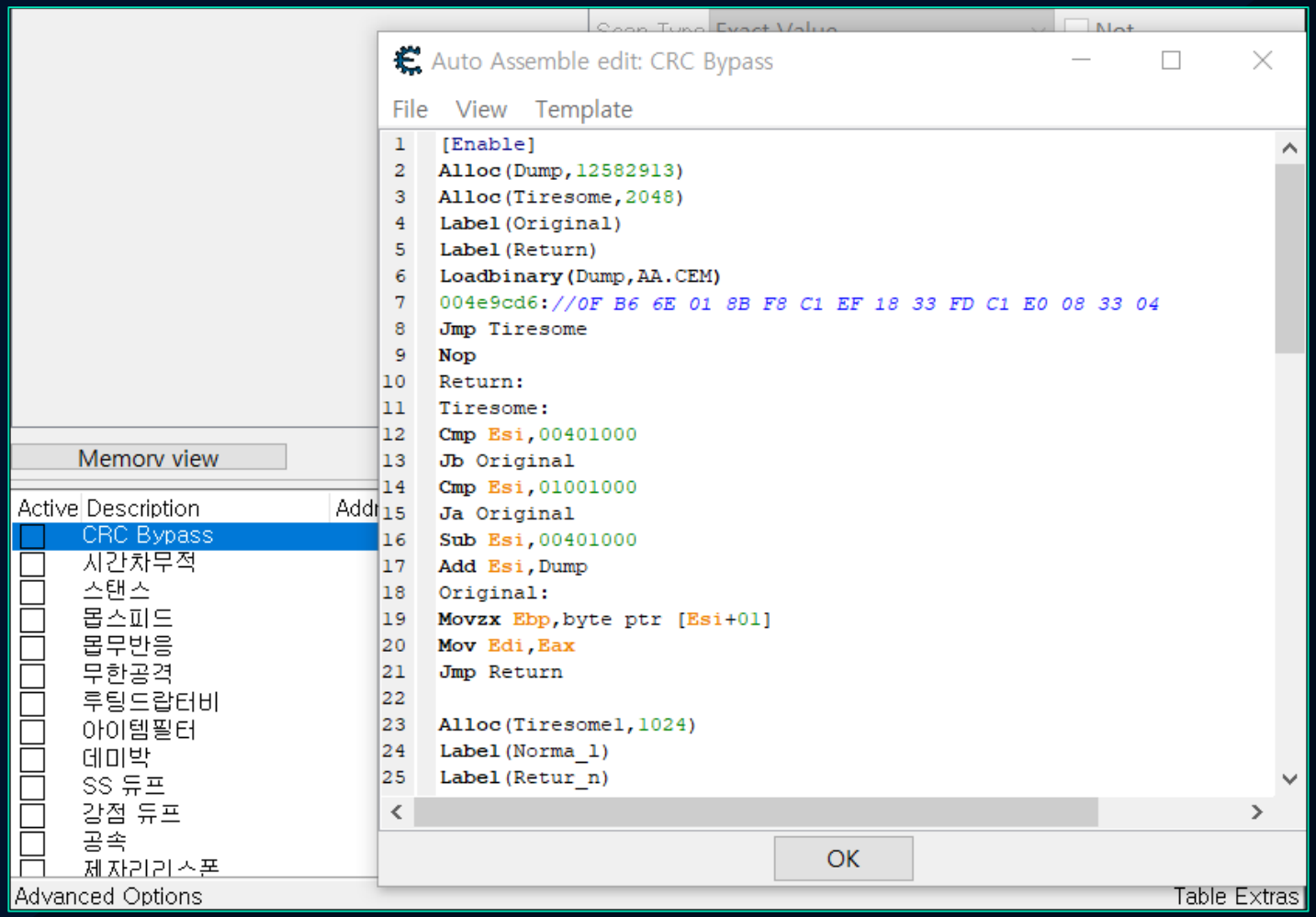

Memory Viewer
File Search View Debug Tools Kernel tools
SuddenAttack.exe+1516
Address Bytes Opcode Comment
SuddenAttack.exe+1516 33 C0 xor eax,eax
SuddenAttack.exe+1518 66 39 05 A0560001 cmp [SuddenAttack.exe+ [00000002]
SuddenAttack.exe+151F 0F94 C0 sete al
SuddenAttack.exe+1522 50 push eax
SuddenAttack.exe+1523 68 09020000 push 00000209 521
SuddenAttack.exe+1528 E8 97270000 call SuddenAttack.exe+3
SuddenAttack.exe+152D 33 C0 xor eax,eax
SuddenAttack.exe+152F 66 83 3D A05600... cmp word ptr [SuddenAtta [00000002]
SuddenAttack.exe+1537 0F94 C0 sete al
SuddenAttack.exe+153A 50 push eax
SuddenAttack.exe+153B 68 0A020000 push 0000020A 522
SuddenAttack.exe+1540 E8 7F270000 call SuddenAttack.exe+3
SuddenAttack.exe+1545 33 C0 xor eax,eax
SuddenAttack.exe+1547 66 83 3D A05600... cmp word ptr [SuddenAtta [00000002]
compare two operands
Protect:Read Only Base=00404000 Size=C1000
address B0 B1 B2 B3 B4 B5 B6 B7 B8 B9 BA BB BC BD BE BF 0123456789ABCDEF
004041B0 00 10 00 00 AF 07 76 02 67 7C 00 00 B8 07 E7 00 .... .v.g|.. . .
004041C0 67 08 00 00 C4 07 E8 00 00 10 00 00 CB 07 E9 00 g... . ...
004041D0 67 04 00 00 87 17 E7 00 67 08 00 80 D2 07 77 02 g... . .g.. .w.
004041E0 0B 00 00 00 D6 07 EA 00 0B 04 00 00 DD 07 78 02 .... .x.
004041F0 64 00 00 00 1F 1B 78 02 64 00 00 80 8E 17 EB 00 d.....x.d.. . .
00404200 64 04 00 80 E2 07 EB 00 64 04 00 00 EA 07 79 02 d.. . .d... .y.
00404210 38 00 00 00 EE 07 EC 00 00 10 00 00 F5 07 ED 00 8... . ...
00404220 38 04 00 00 FC 07 7A 02 0C 00 00 00 00 08 EE 00 8... .z..... .
00404230 0C 1C 00 00 08 08 EF 00 0C 08 00 00 0F 08 F0 00 ....
00404240 00 10 00 00 16 08 F1 00 00 10 00 00 1D 08 F2 00 ....

HACKING

CRC - BYPASS

HACKING

CRC - BYPASS

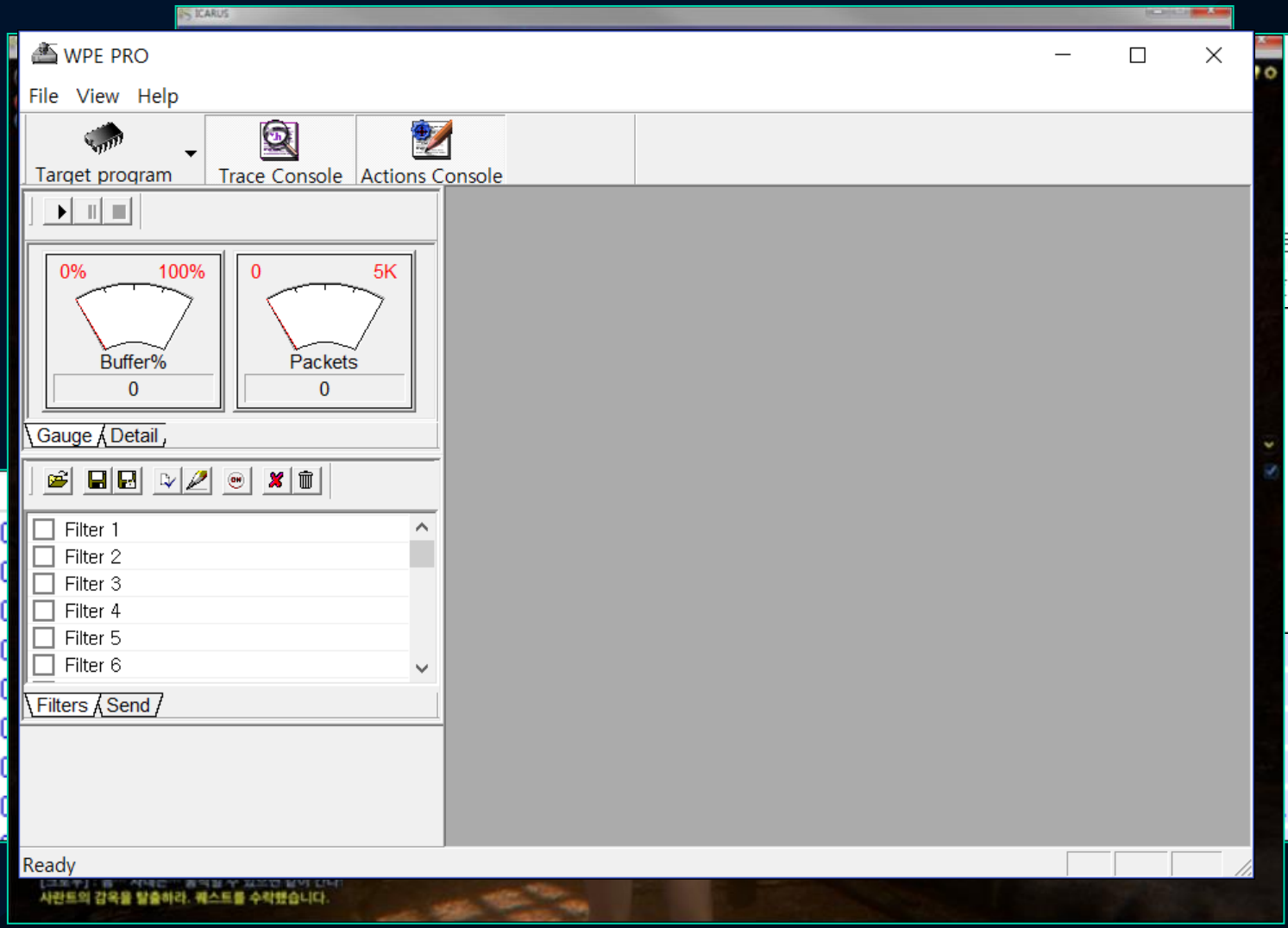


HACKING

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;
    }
```

PACKET



HACKING

NoN-Client Bot

HOOKING

HOOKING

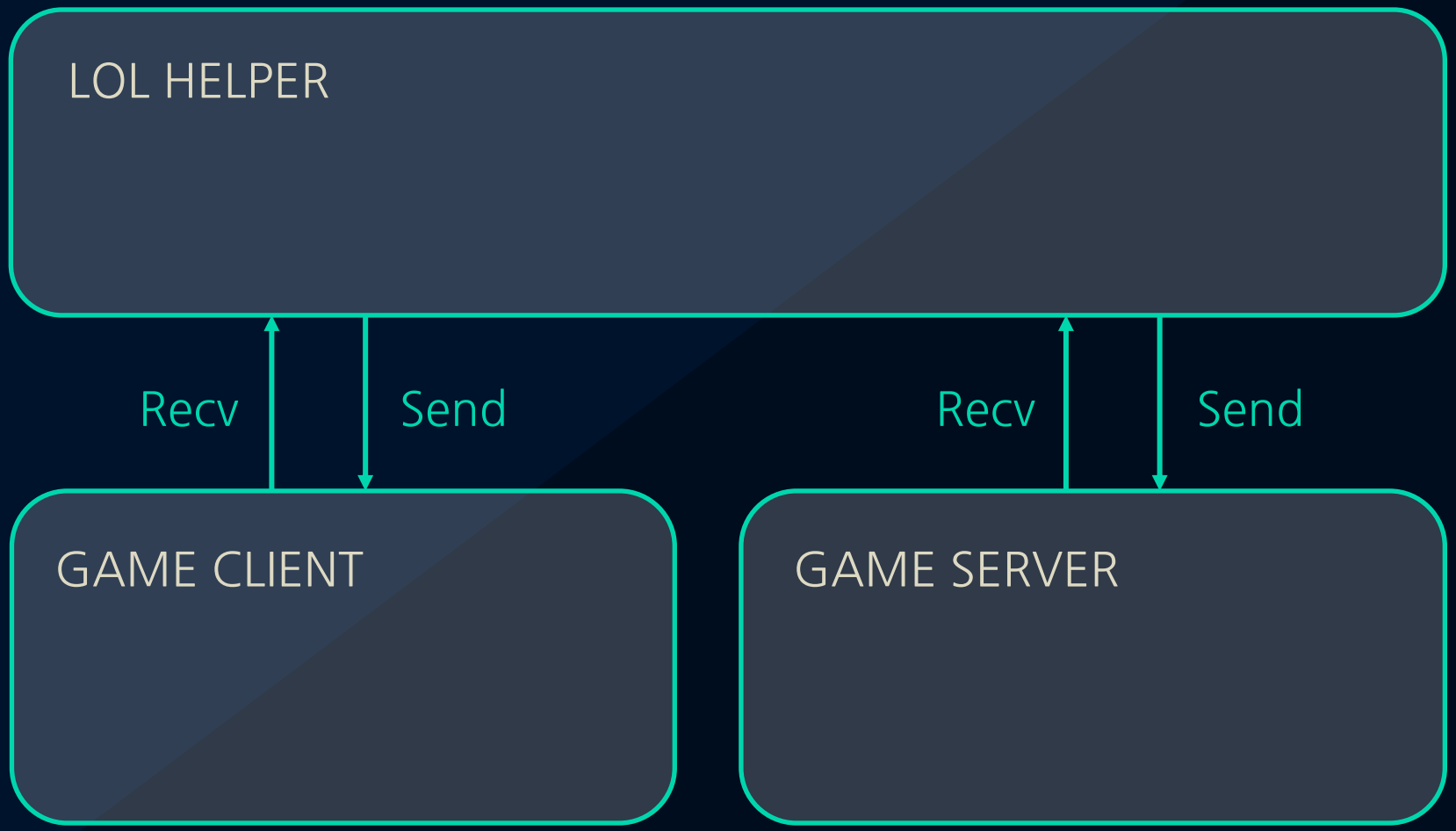
01. Connect 함수를 후킹

02. 내 프로그램의 소켓으로 연결

03. 내 소켓에서 패킷을 복호화하고
    원하는 대로 패킷을 변조

04. 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

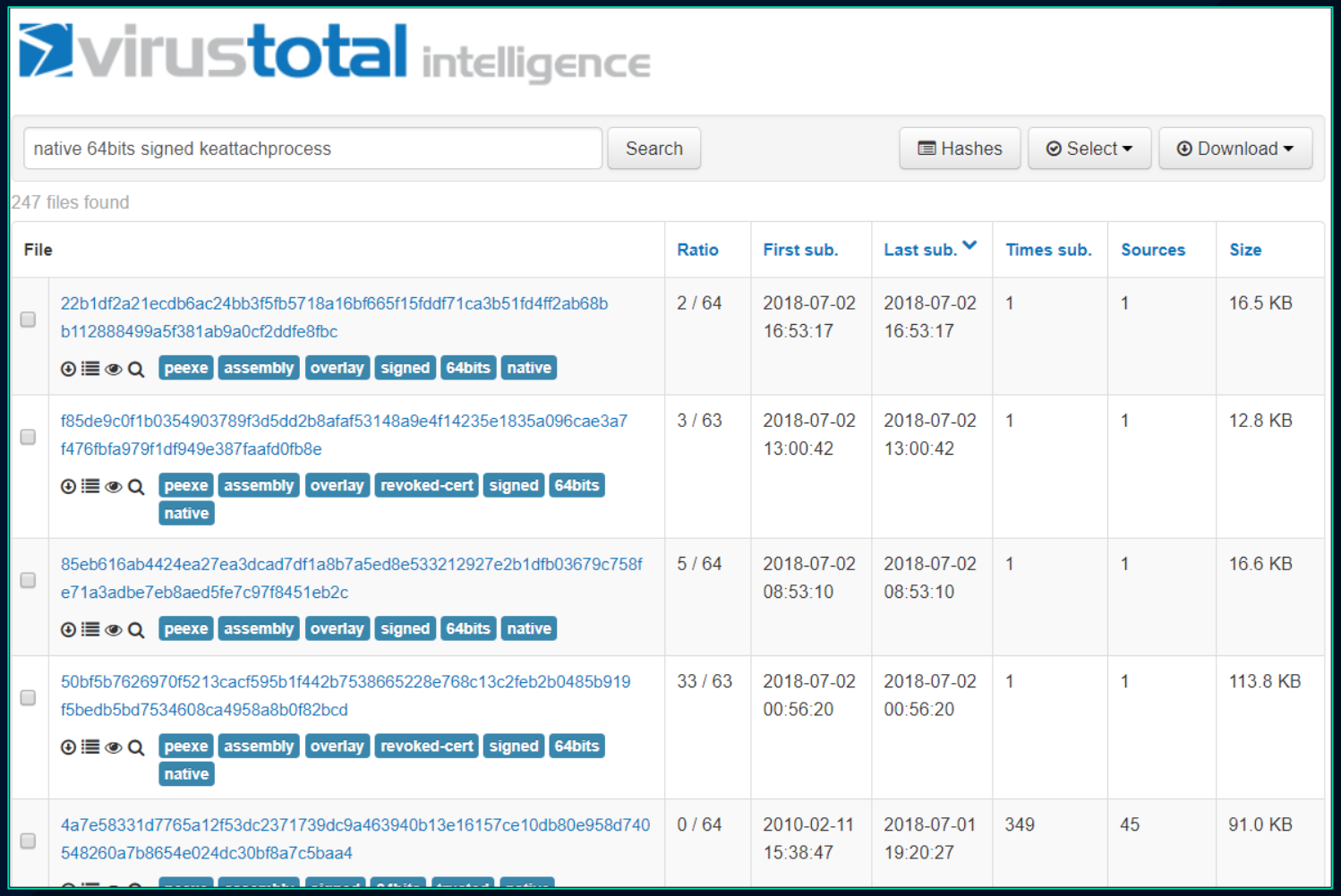
HACKING

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=%pWn", v12);
      if ( v12 )
        v7 = 0xC0000001;
    }
  }
  KeDetachProcess();
  ObfDereferenceObject(Object);
  result = (v7 & 0x80000000) == 0;
}
```

HACKING

DRIVER



HACKING

SECURITY

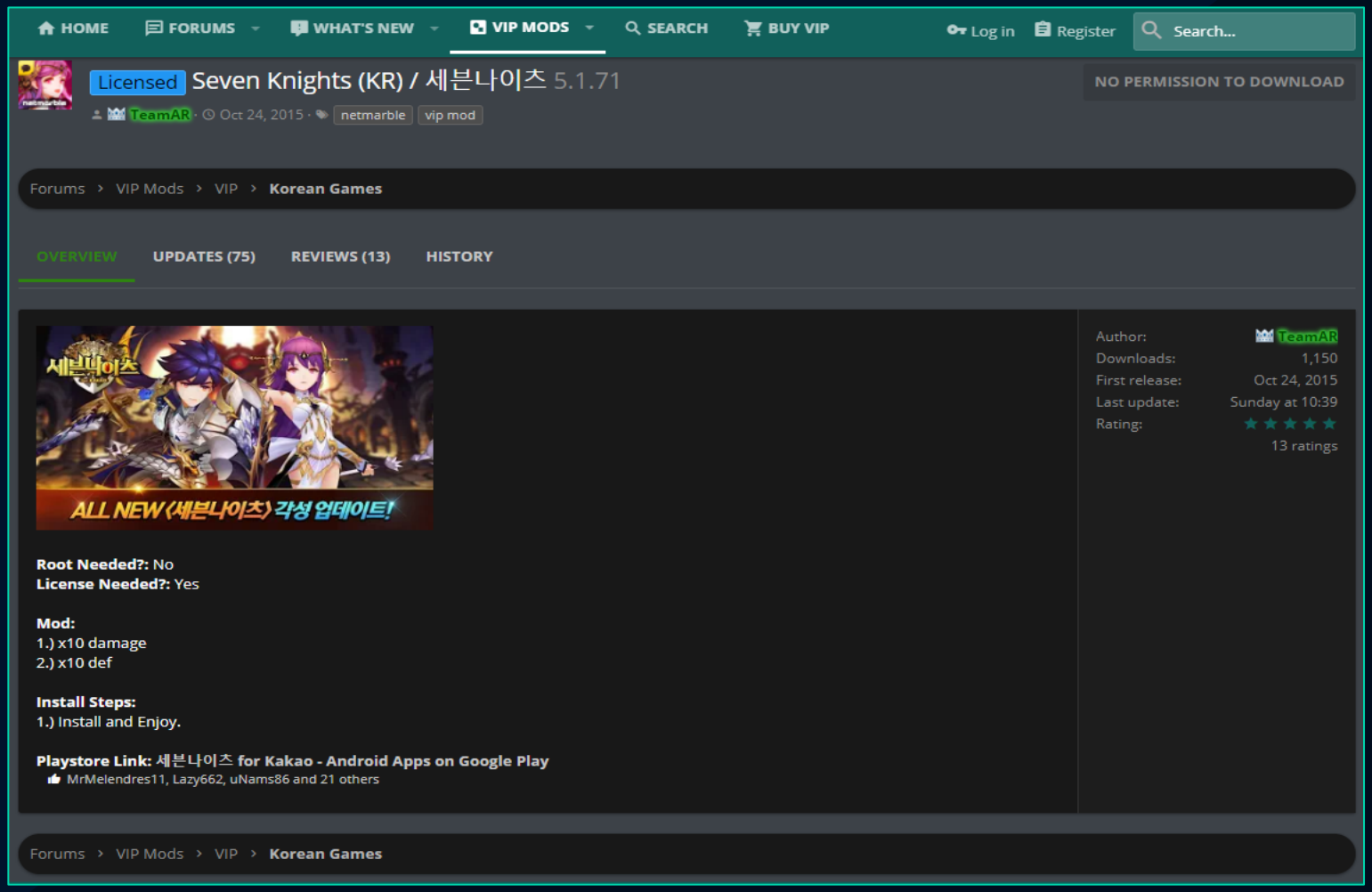
XIGNCODE3
Copyright(C) 2015 Wellbia.com Co., Ltd
All rights reserved

AhnLab
HackShield Pro
for Online Game
Copyright(c). AhnLab, Inc. 2002-2006. All rights reserved.

X-TRAP
X-TRAP Web Management System

INCA
nProtect GameGuard
No.1 Global Game Security Solution

MOBILE


HOME
FORUMS
WHAT'S NEW
VIP MODS
SEARCH
BUY VIP
Log in
Register
Search...
Licensed Seven Knights (KR) / 세븐나이츠 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 〈세븐나이츠〉 각성 업데이트!
Author: TeamAR
Downloads: 1,150
First release: Oct 24, 2015
Last update: Sunday at 10:39
Rating:
13 ratings
Root Needed?: No
License Needed?: Yes
Mod:
1.) x10 damage
2.) x10 def
Install Steps:
1.) Install and Enjoy.
Playstore Link: 세븐나이츠 for Kakao - Android Apps on Google Play
MrMelendres11, Lazy662, uNams86 and 21 others
Forums › VIP Mods › VIP › Korean Games

끝으로...

Q&A

HACKING