ON-LINE GAME HACKING

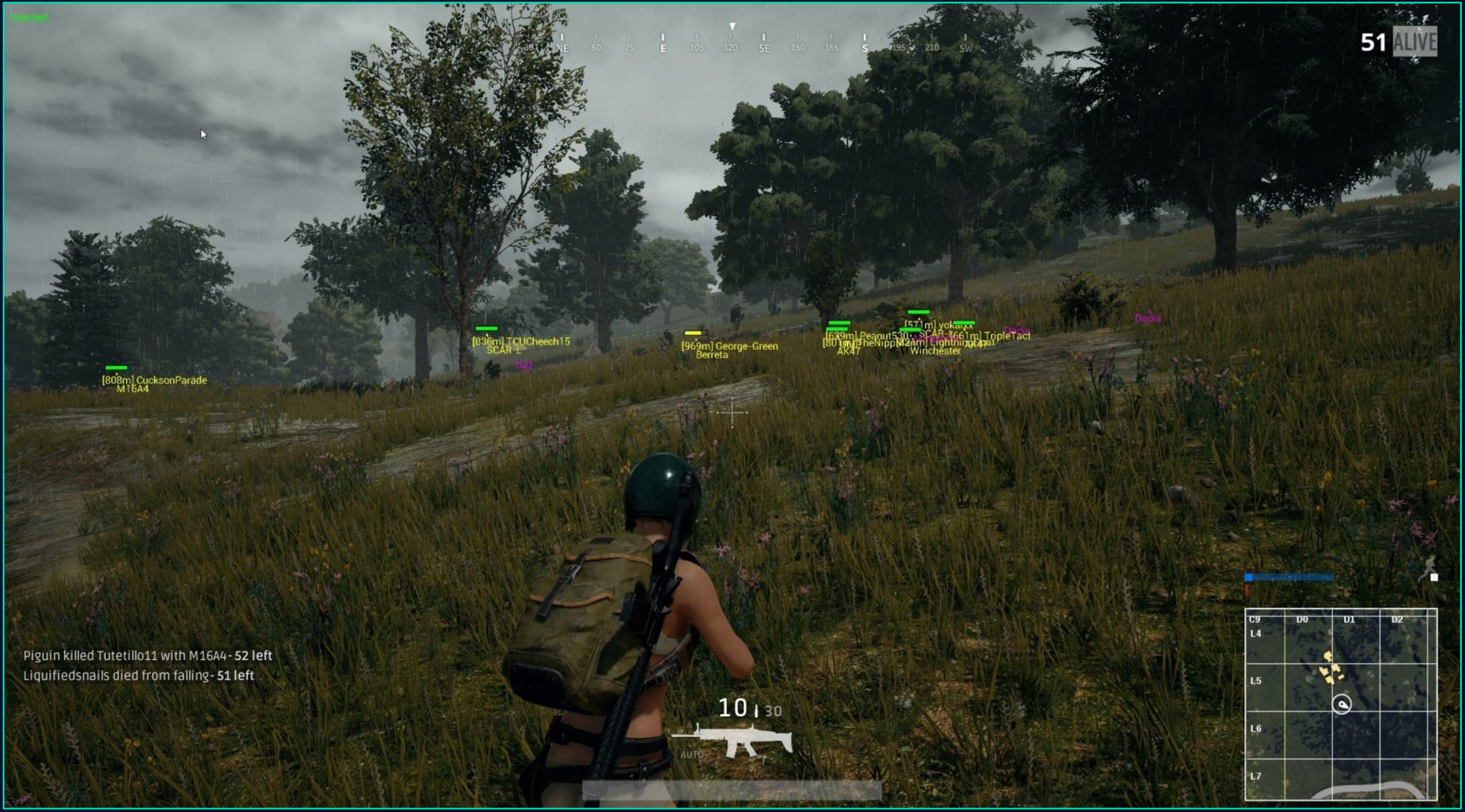
강민수(강명석) admin@hack.kr

HACKING

www.CodeEngn.com
2018 CodeEngn Conference 15

Code Engn

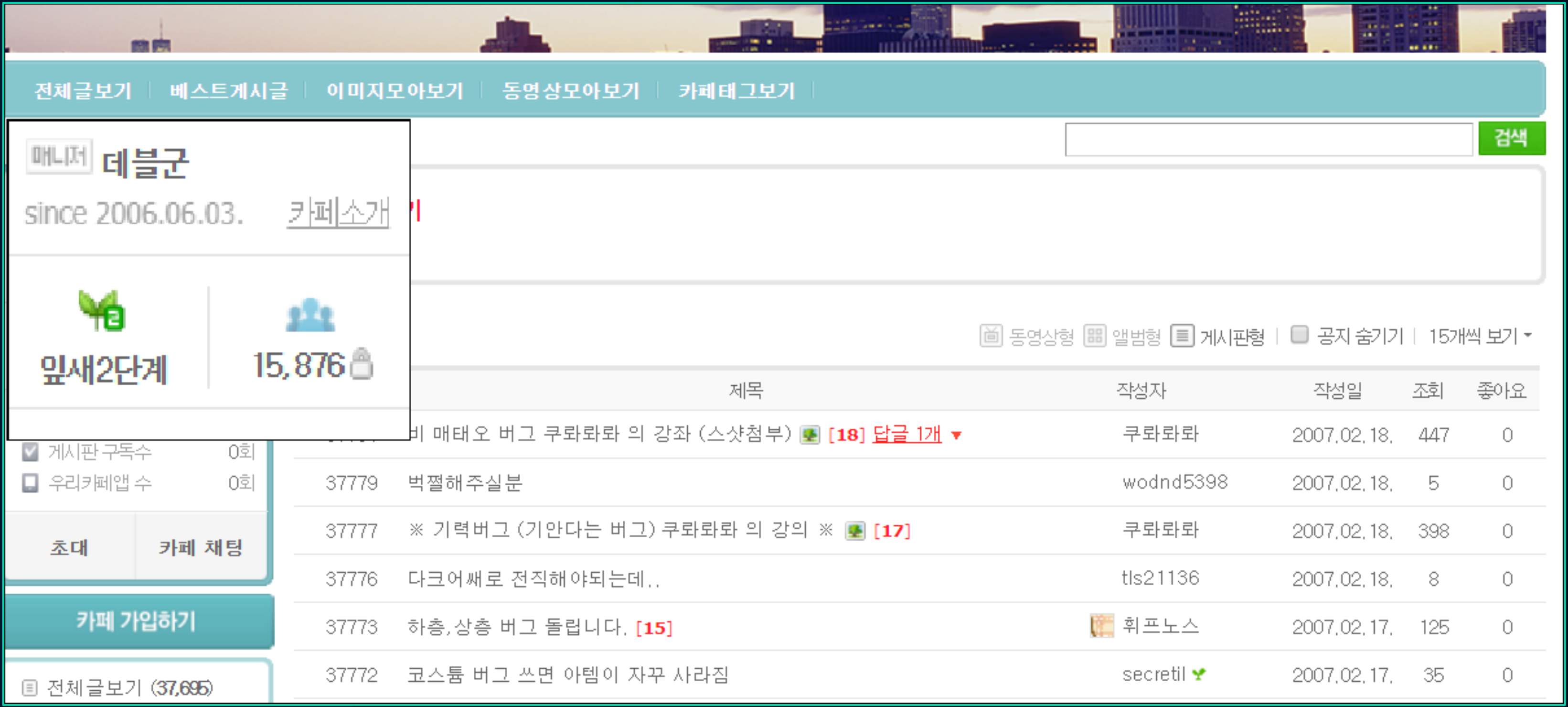
GAME HACK



Piguin killed Tutetillo11 with M16A4 - 52 left
Liquifiedsnails died from falling - 51 left

HACKING

CULTURE



매니저 데블군

since 2006.06.03. 카페소개

잎새2단계

15,876

☑ 게시판 구독수 0회

□ 우리카페앱 수 0회

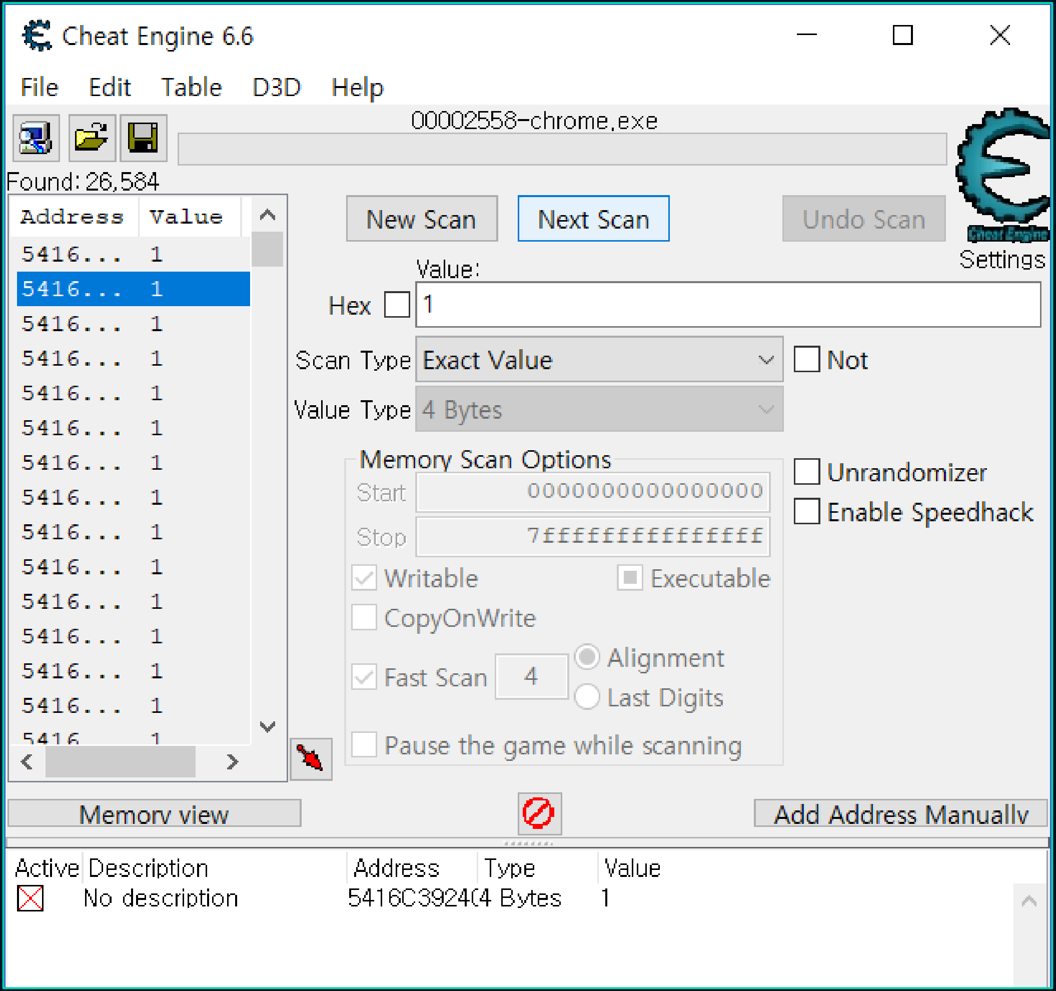
전체글보기 (37,695)

동영상형 앨범형 게시판형 | □ 공지 숨기기 | 15개씩 보기

	제목	작성자	작성일	조회	좋아요
	비 매태오 버그 쿠롸롸롸 의 강좌 (스샷첨부) [18] 답글 1개	쿠롸롸롸	2007.02.18.	447	0
37779	벅쩔해주실분	wodnd5398	2007.02.18.	5	0
37777	※ 기력버그 (기안다는 버그) 쿠롸롸롸 의 강의 ※ [17]	쿠롸롸롸	2007.02.18.	398	0
37776	다크어쌔로 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	secretil	2007.02.17.	35	0

HACKING

CHEAT ENGINE



00002558-chrome.exe

Found: 26,584

Address	Value
5416...	1
5416...	1
5416...	1
5416...	1
5416...	1
5416...	1
5416...	1
5416...	1
5416...	1
5416...	1
5416...	1
5416...	1
5416...	1
5416...	1
5416	1

Value: 1

Hex □

Scan Type: Exact Value □ Not

Value Type: 4 Bytes

Memory Scan Options

Start 0000000000000000

Stop 7fffffffffffffff

☑ Writable ▣ Executable

□ CopyOnWrite

☑ Fast Scan 4 ● Alignment ○ Last Digits

□ Pause the game while scanning

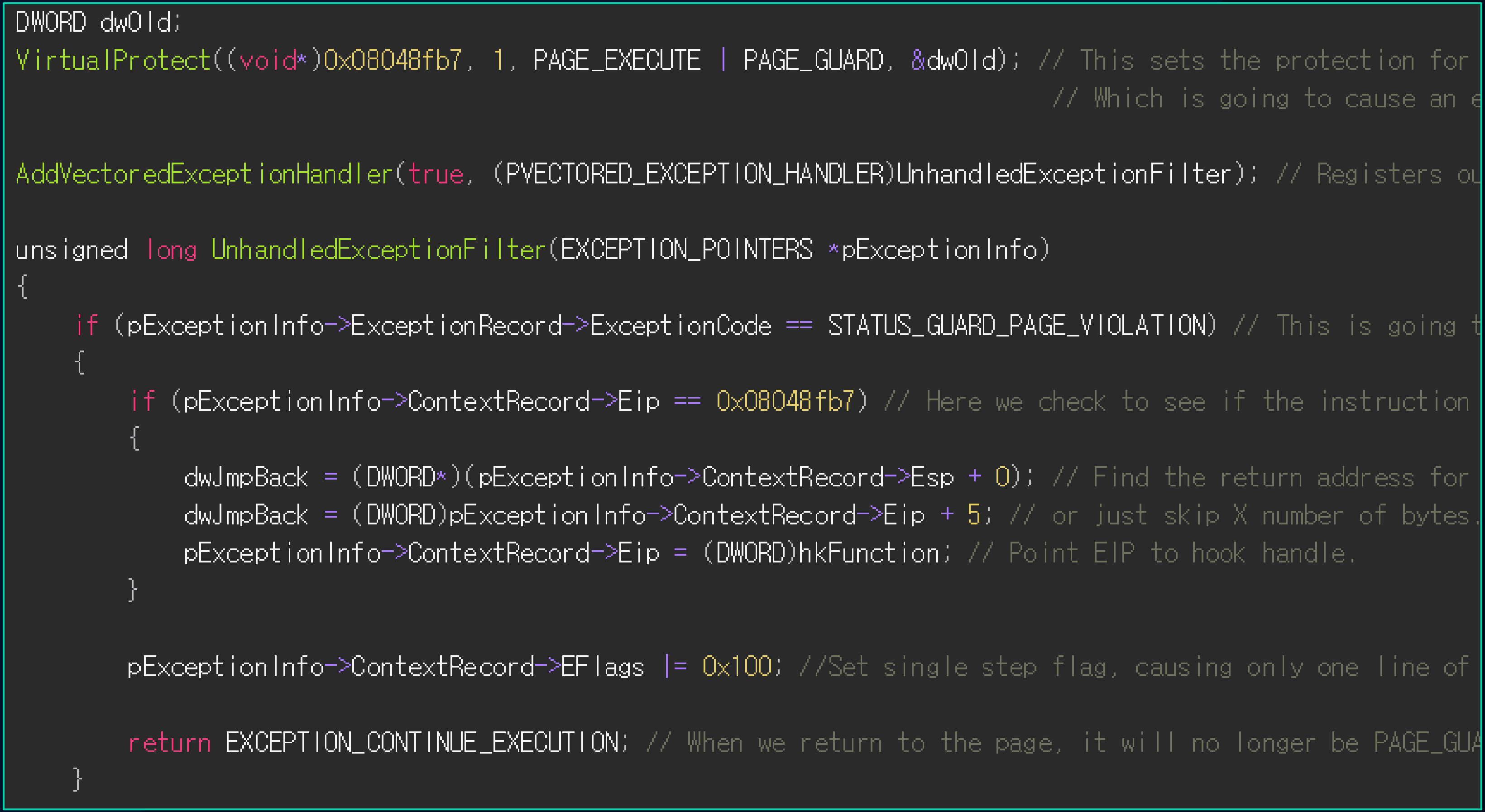
□ Unrandomizer

□ Enable Speedhack

Active	Description	Address	Type	Value
☒	No description	5416C3924(	4 Bytes	1

HACKING

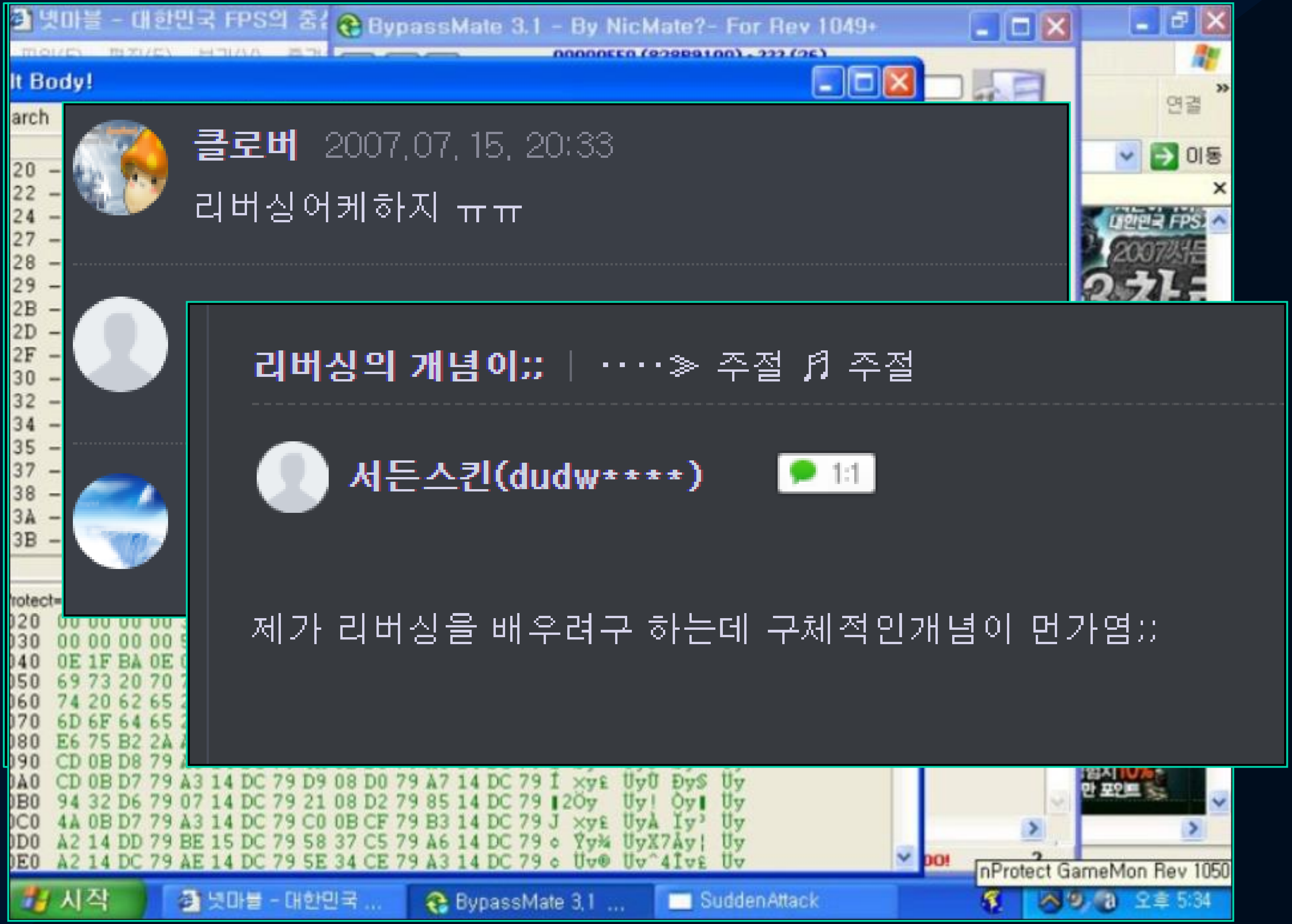
CHEAT ENGINE



```
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


넷마블 - 대한민국 FPS의 중
BypassMate 3.1 - By NicMate?- For Rev 1049+
lt Body!
arch
연결
이동
시작
넷마블 - 대한민국 ...
BypassMate 3.1 ...
SuddenAttack
nProtect GameMon Rev 1050
오후 5:34

클로버 2007.07.15. 20:33

리버싱어케하지 ㅠㅠ

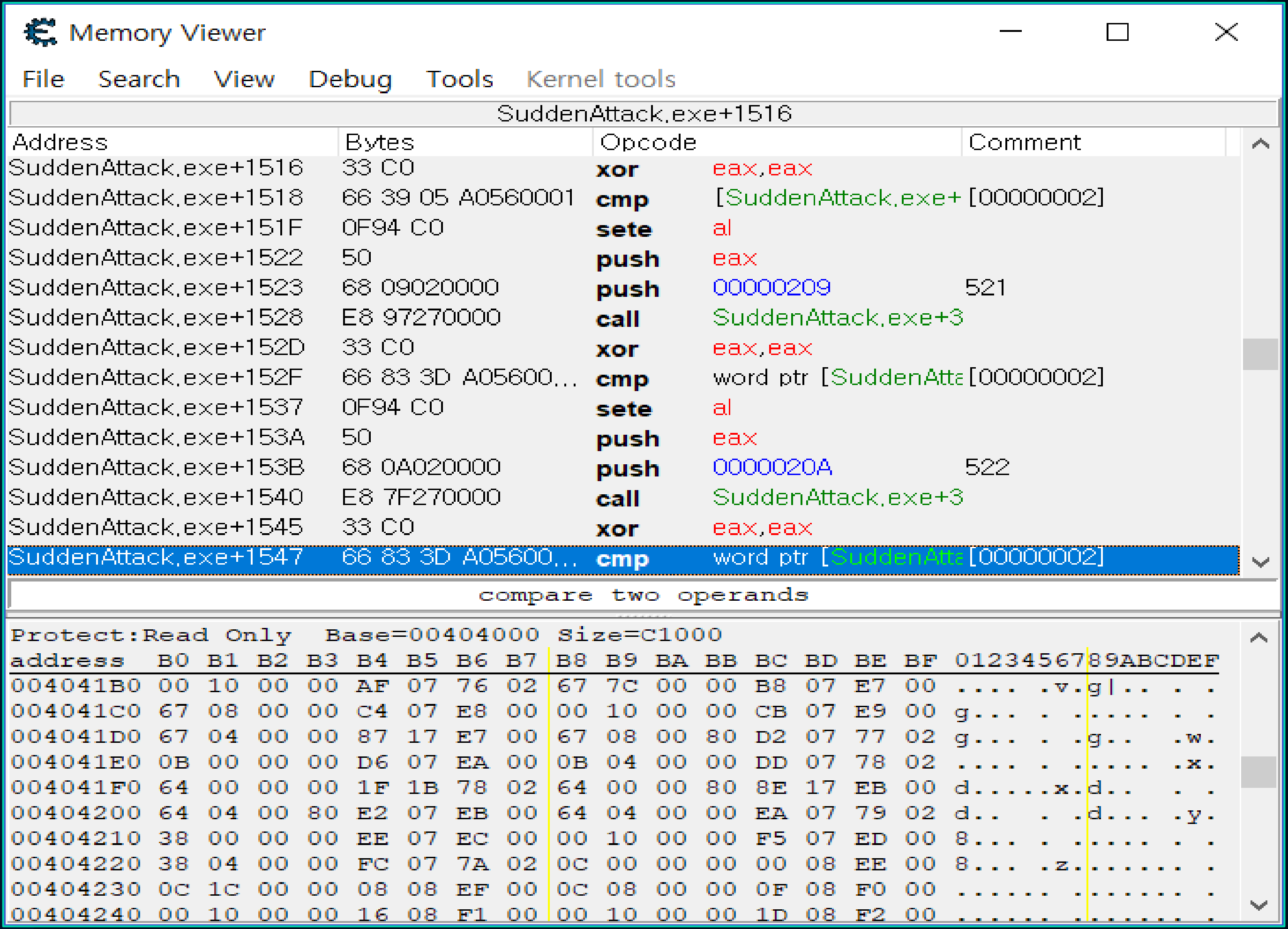
리버싱의 개념이;; | ····≫ 주절 ♬ 주절

서든스킨(dudw**)** 1:1

제가 리버싱을 배우려구 하는데 구체적인개념이 먼가염;;

HACKING

CRC

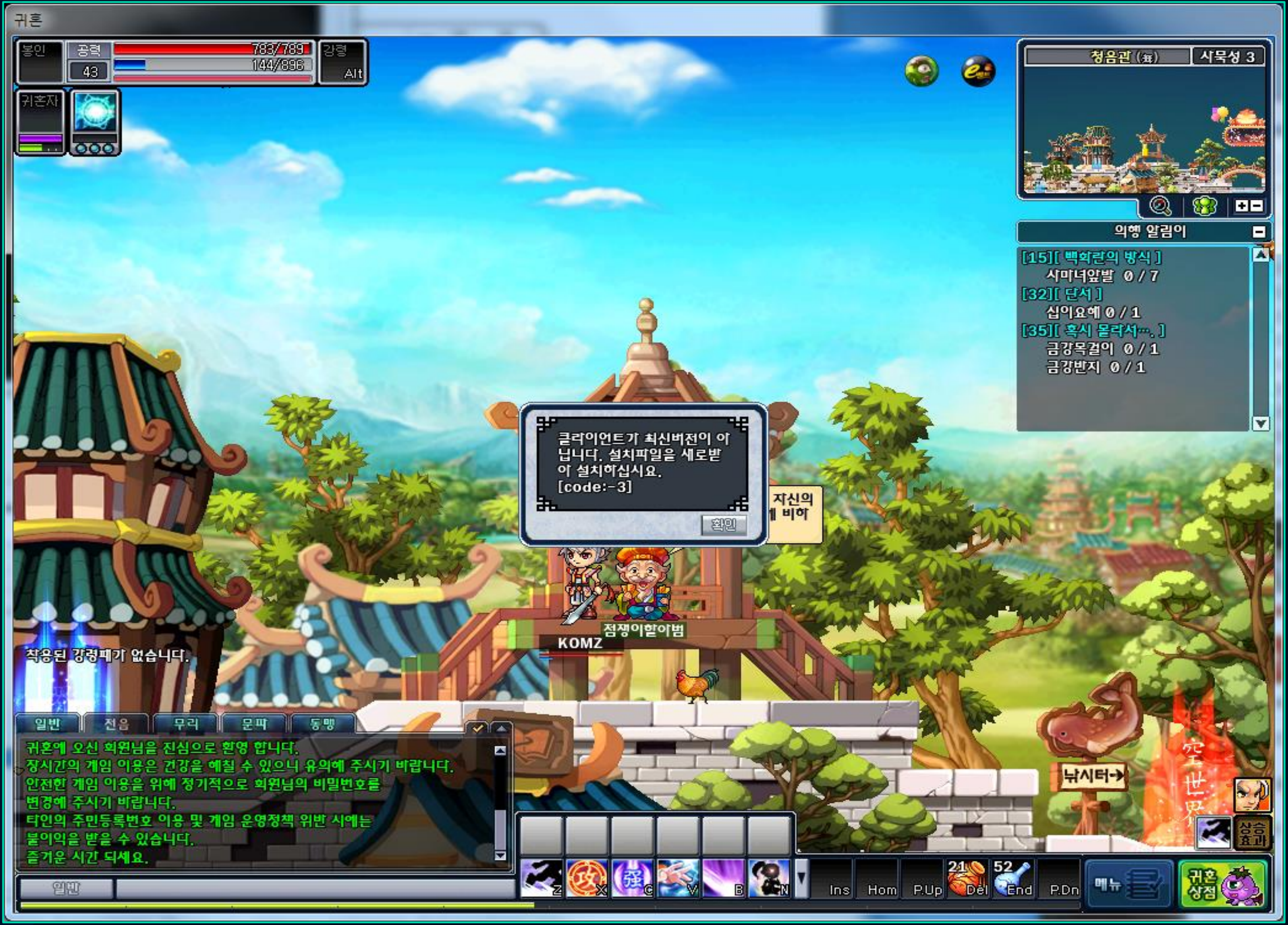


```
SuddenAttack.exe+1516
Address                 Bytes                Opcode                         Comment
SuddenAttack.exe+1516   33 C0                xor    eax,eax
SuddenAttack.exe+1518   66 39 05 A0560001    cmp    [SuddenAttack.exe+[00000002]
SuddenAttack.exe+151F   0F94 C0              sete   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



클라이언트가 최신버전이 아닙니다. 설치파일을 새로받아 설치하십시요.
[code:-3]

착용된 강령패가 없습니다.

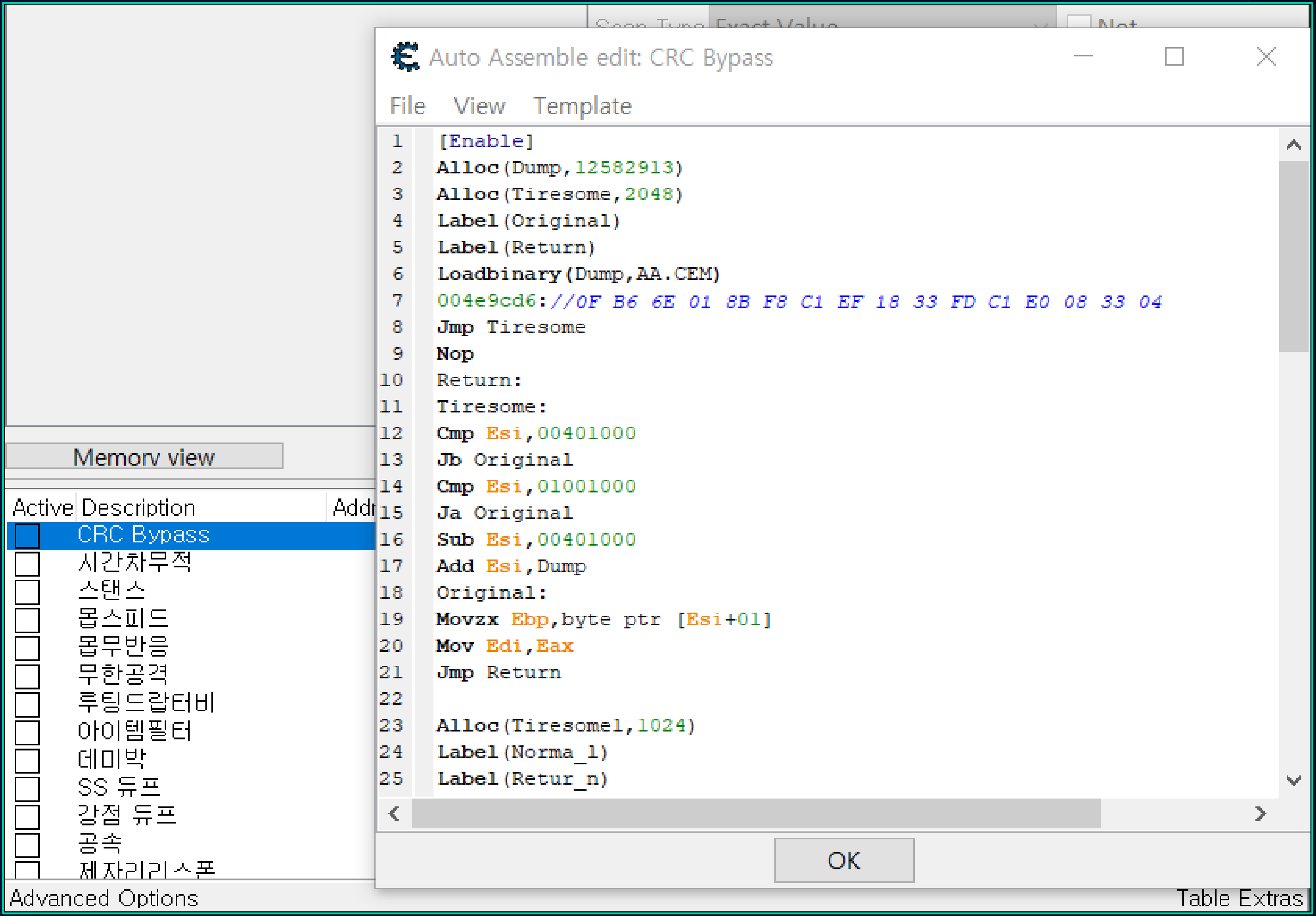
귀혼에 오신 회원님을 진심으로 환영 합니다.
장시간의 게임 이용은 건강을 해칠 수 있으니 유의해 주시기 바랍니다.
안전한 게임 이용을 위해 정기적으로 회원님의 비밀번호를 변경해 주시기 바랍니다.
타인의 주민등록번호 이용 및 게임 운영정책 위반 시에는 불이익을 받을 수 있습니다.
즐거운 시간 되세요.

의행 알림이

[15][백화란의 방식]
사마녀앞발 0 / 7
[32][단서]
십이요혜 0 / 1
[35][혹시 몰라서….]
금강목걸이 0 / 1
금강반지 0 / 1

HACKING

CRC - BYPASS

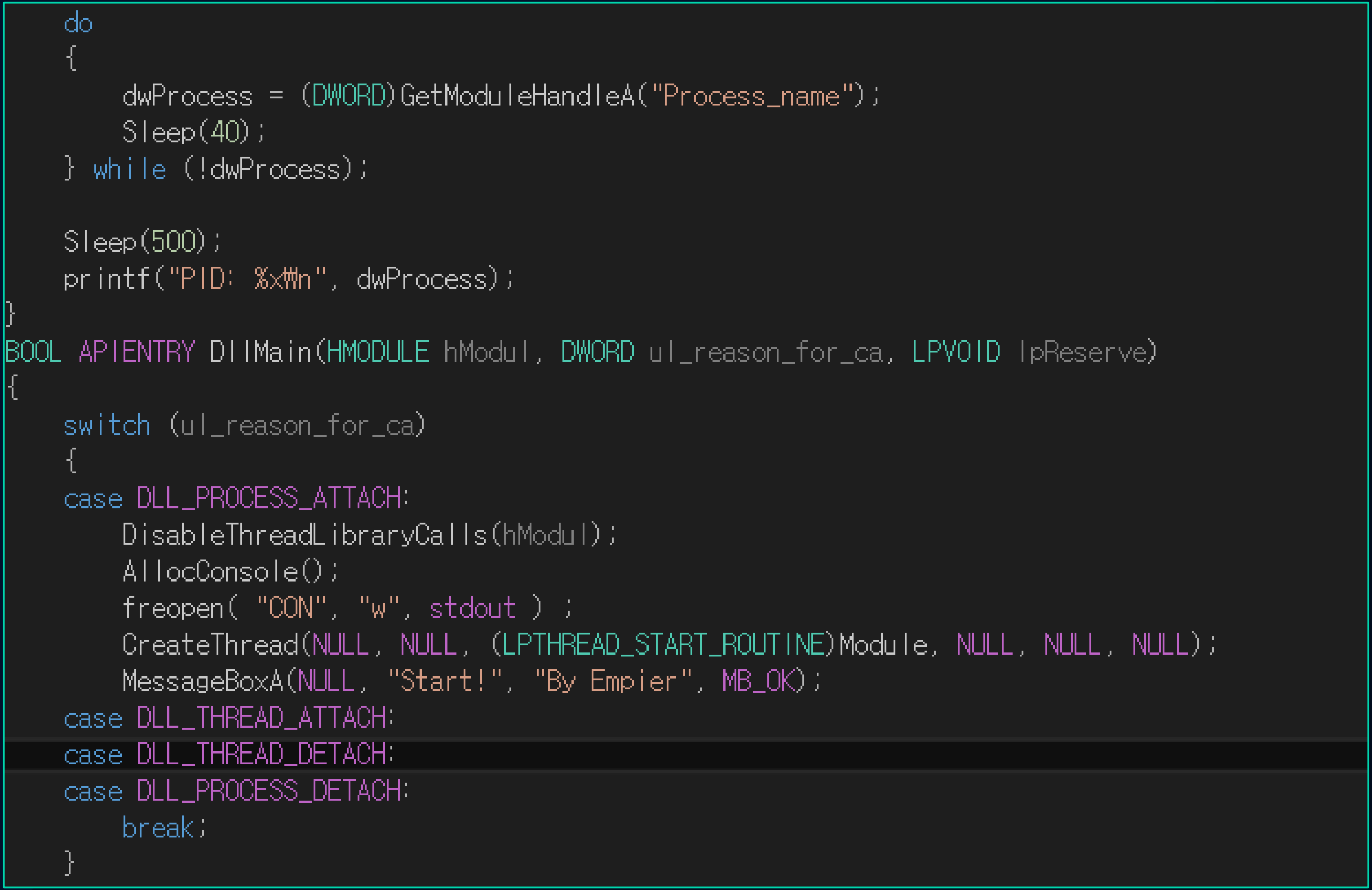


```
[Enable]
Alloc(Dump,12582913)
Alloc(Tiresome,2048)
Label(Original)
Label(Return)
Loadbinary(Dump,AA.CEM)
004e9cd6://0F B6 6E 01 8B F8 C1 EF 18 33 FD C1 E0 08 33 04
Jmp Tiresome
Nop
Return:
Tiresome:
Cmp Esi,00401000
Jb Original
Cmp Esi,01001000
Ja Original
Sub Esi,00401000
Add Esi,Dump
Original:
Movzx Ebp,byte ptr [Esi+01]
Mov Edi,Eax
Jmp Return

Alloc(Tiresome1,1024)
Label(Norma_l)
Label(Retur_n)
```

Active	Description	Addr
□	CRC Bypass	
□	시간차무적	
□	스탠스	
□	몹스피드	
□	몹무반응	
□	무한공격	
□	루팅드랍터비	
□	아이템필터	
□	데미박	
□	SS 듀프	
□	강점 듀프	
□	공속	
□	제자리리스폰	

H
A
C
K
I
N
G

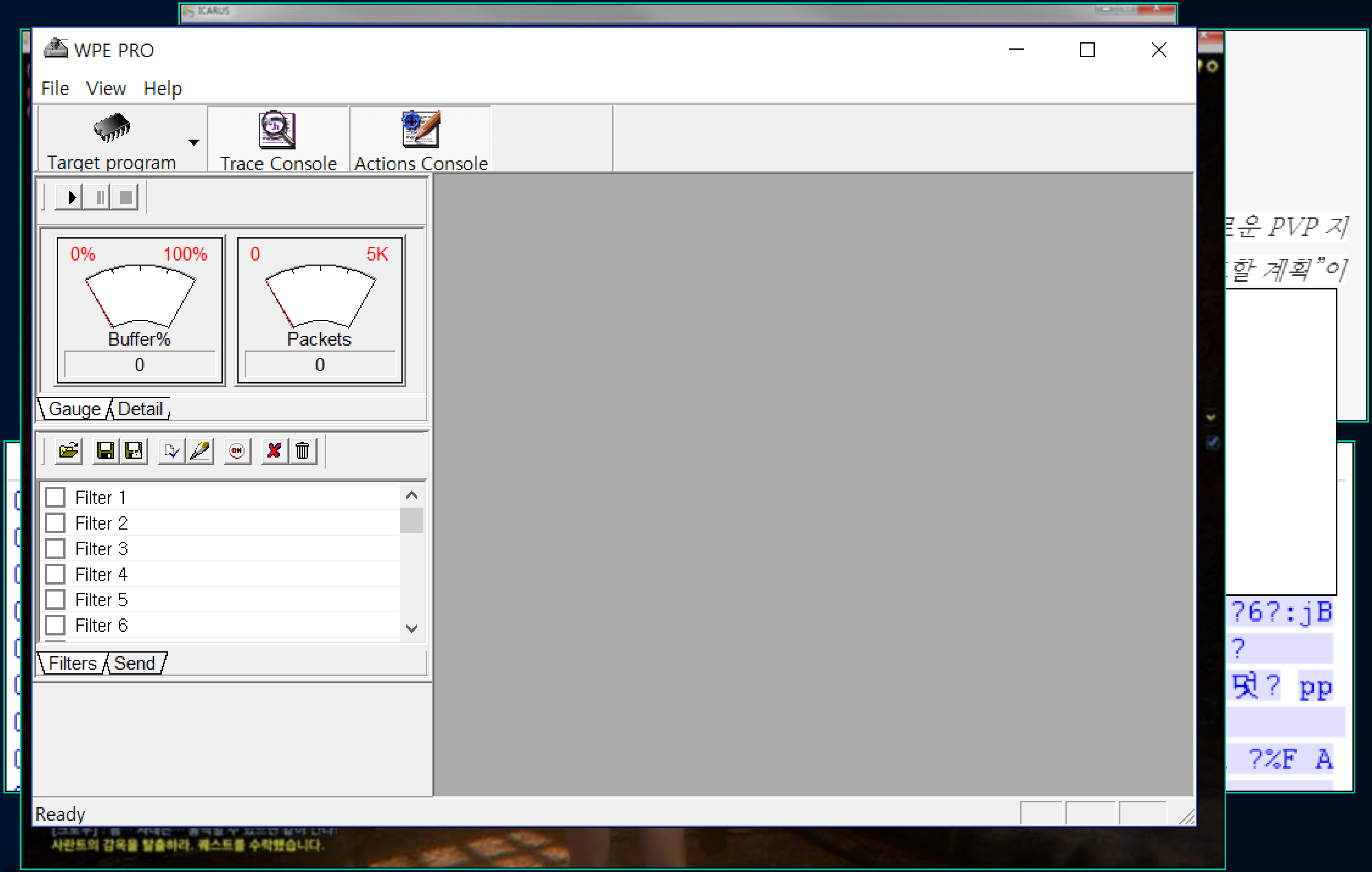
DLL INJECTION



```
    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;
    }
```

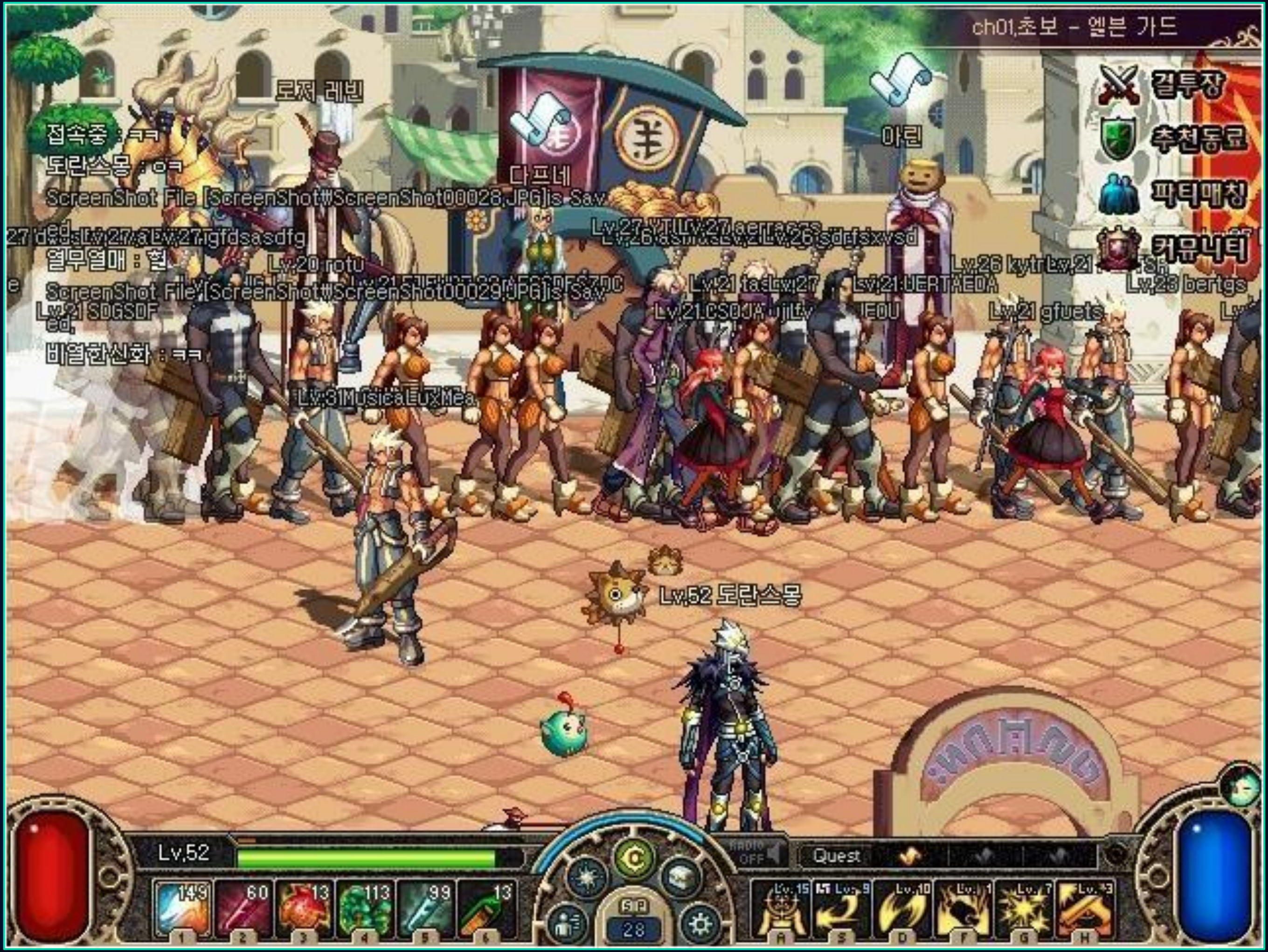
HACKING

PACKET



HACKING

NoN-Client Bot



접속중 : ㅋㅋ

도란스몽 : ㅇㅋ

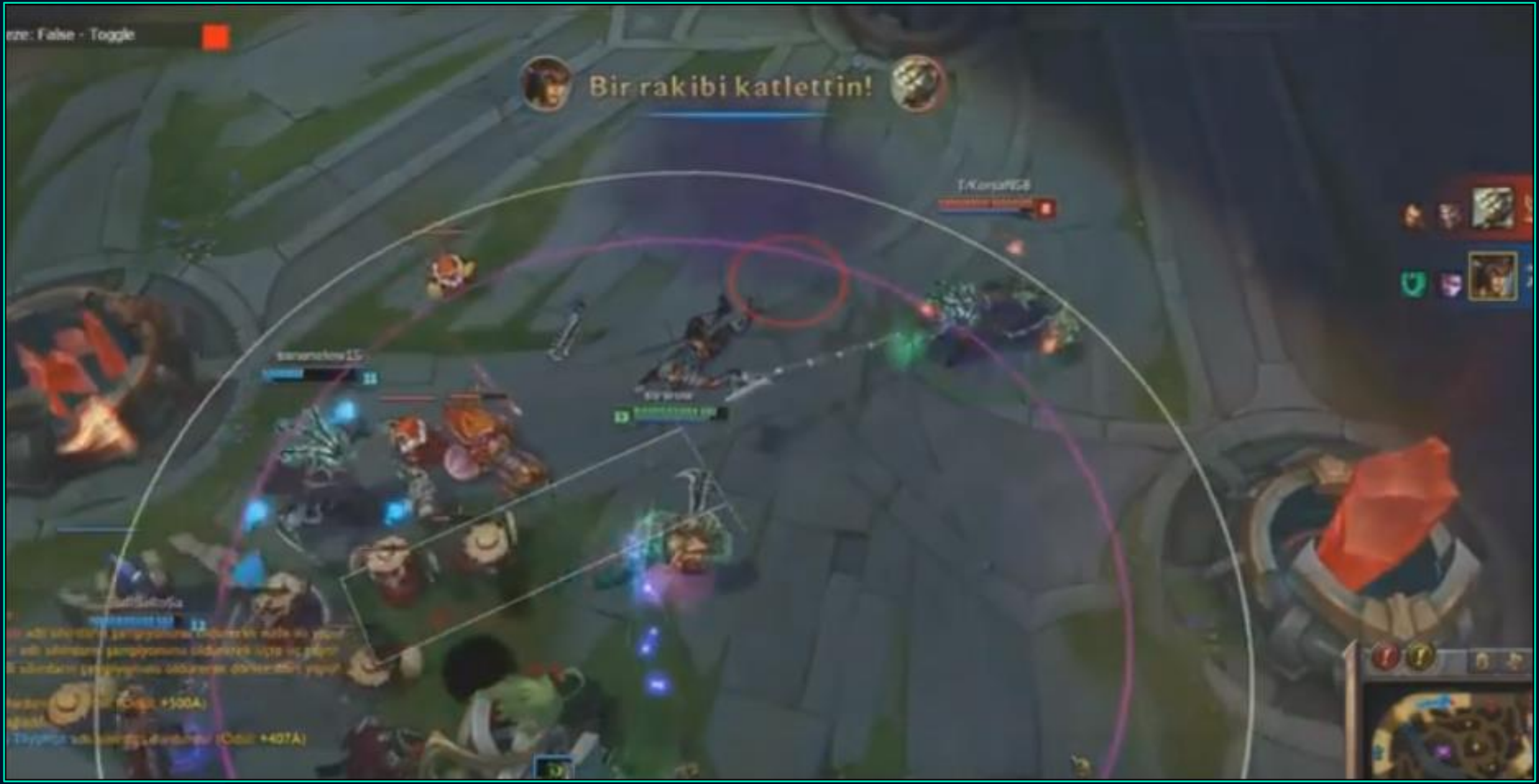
ScreenShot File [ScreenShot#ScreenShot00028.JPG]is Sav

열무열매 : 헐

ScreenShot File [ScreenShot#ScreenShot00029.JPG]is Sav

비열한신화 : ㅋㅋ

HOOKING



eze: False - Toggle

Bir rakibi katlettin!

HOOKING

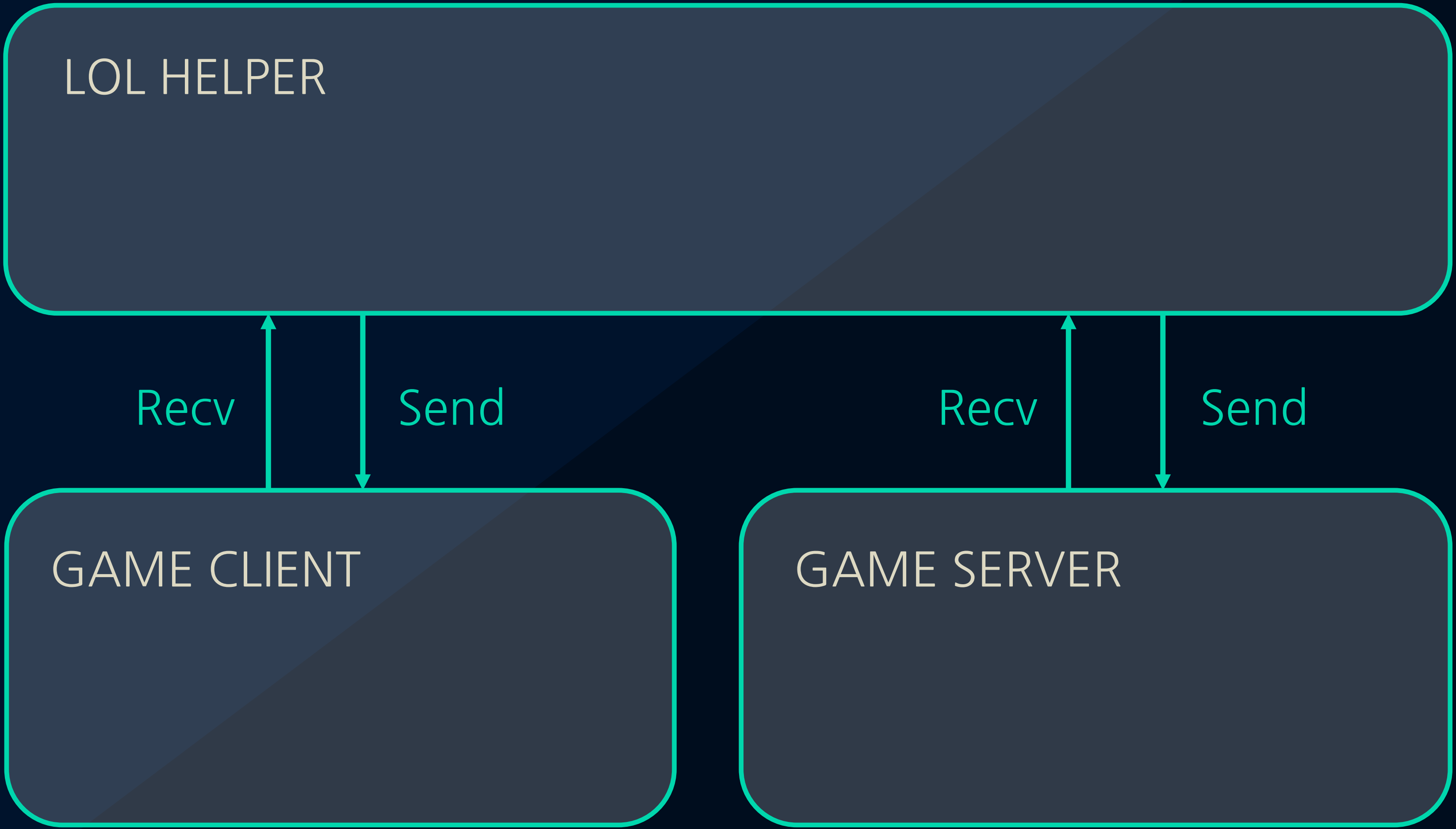
01. Connect 함수를 후킹

02. 내 프로그램의 소켓으로 연결

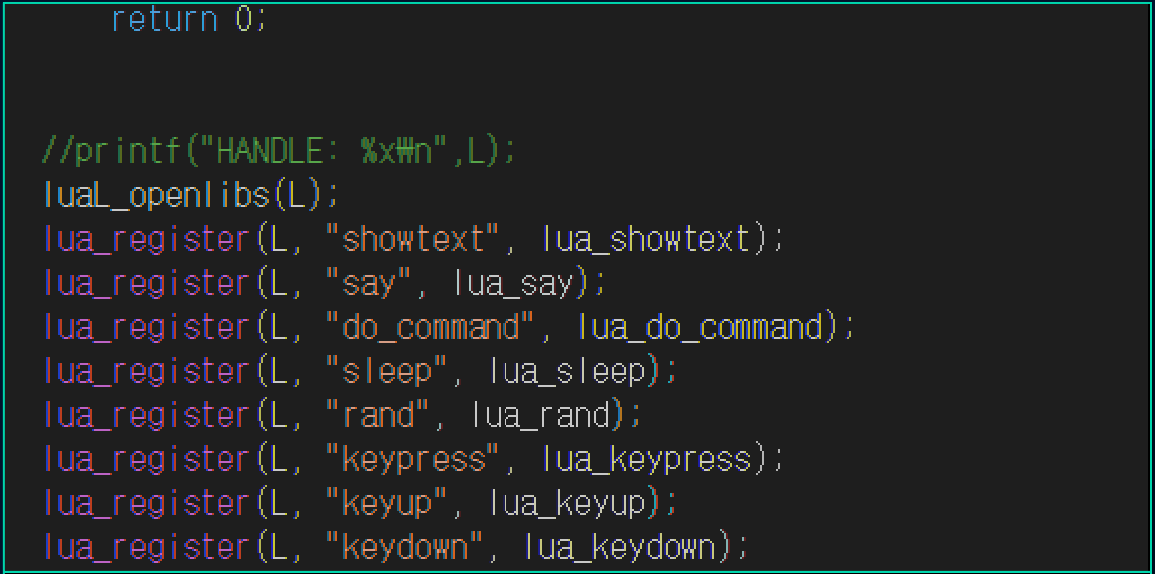
03. 내 소켓에서 패킷을 복호화하고
원하는 대로 패킷을 변조

04. 다시 암호화 하여 원래 목적지로 전송

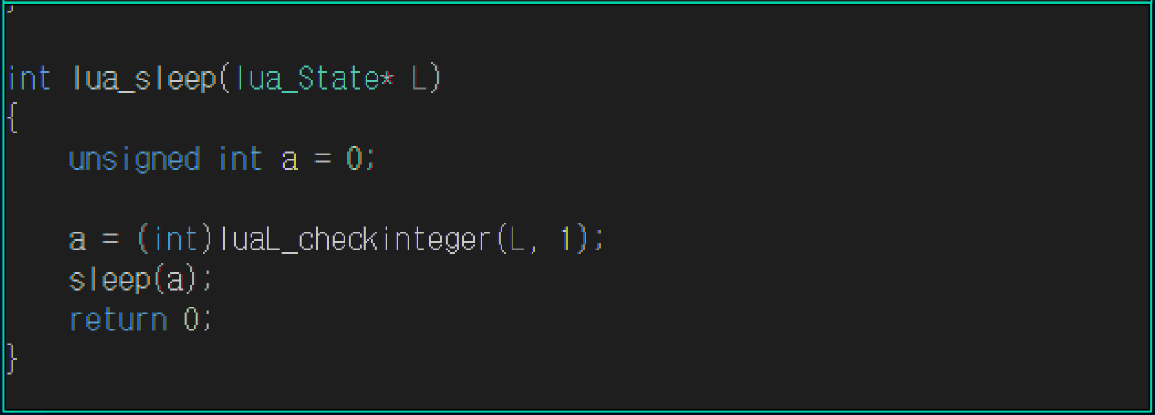
HOOKING



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);
```



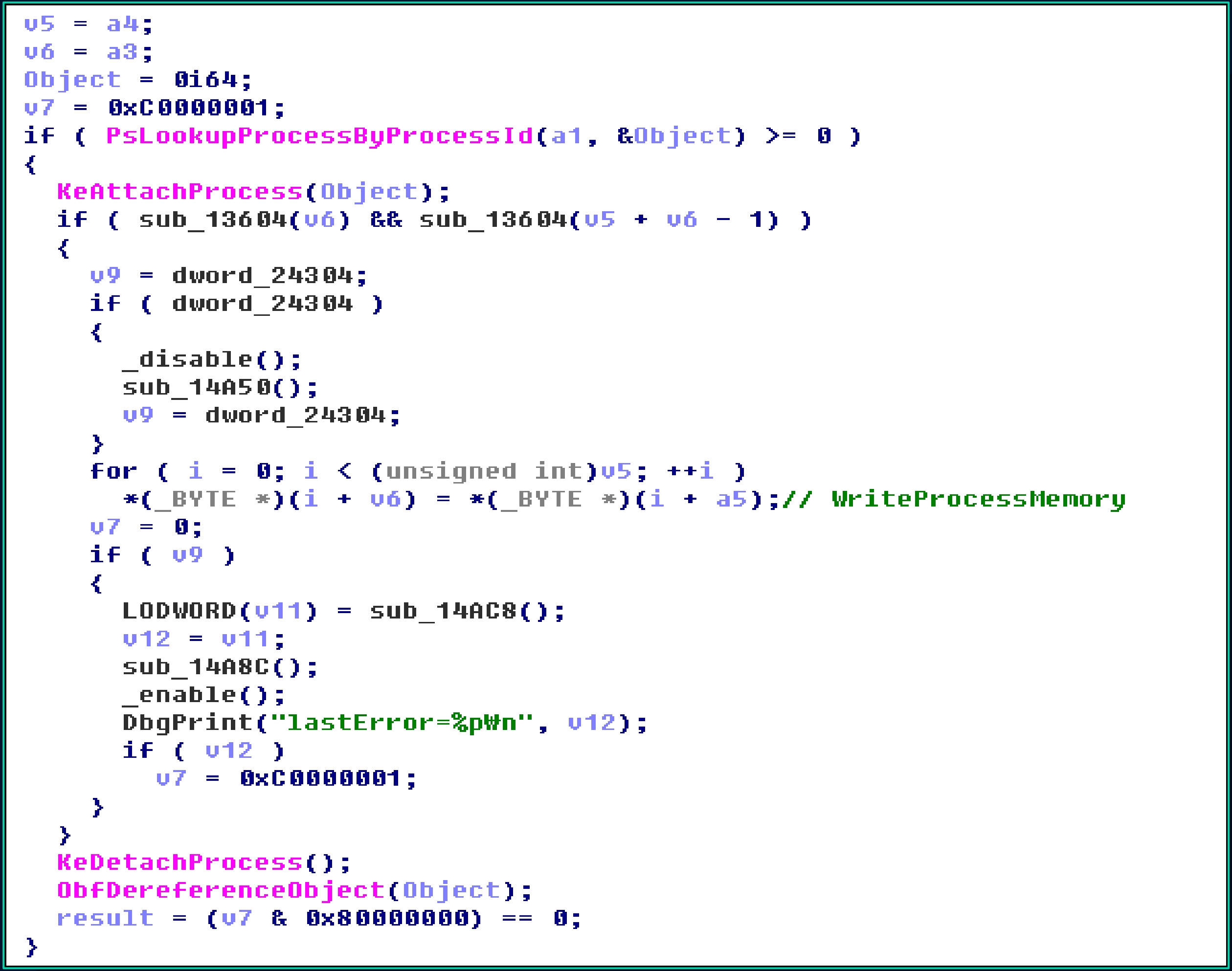
```
int lua_sleep(lua_State* L)
{
    unsigned int a = 0;

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

HACKING

DEMO

HACKING

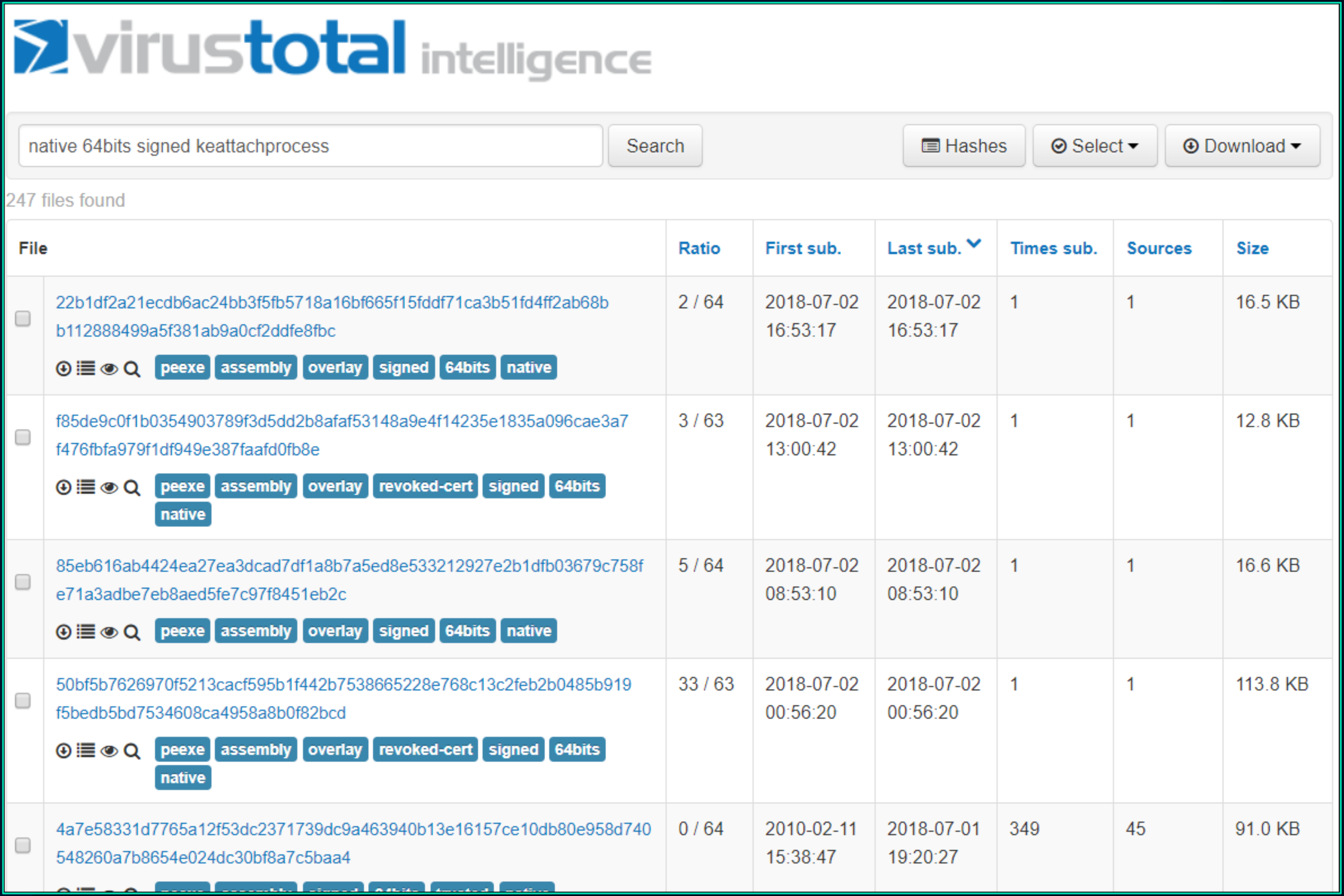
DRIVER



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

HACKING

DRIVER



virustotal intelligence

247 files found

	File	Ratio	First sub.	Last sub.	Times sub.	Sources	Size
□	22b1df2a21ecdb6ac24bb3f5fb5718a16bf665f15fddf71ca3b51fd4ff2ab68b b112888499a5f381ab9a0cf2ddfe8fbc peexe assembly overlay signed 64bits native	2 / 64	2018-07-02 16:53:17	2018-07-02 16:53:17	1	1	16.5 KB
□	f85de9c0f1b0354903789f3d5dd2b8afaf53148a9e4f14235e1835a096cae3a7 f476fbfa979f1df949e387faafd0fb8e peexe assembly overlay revoked-cert signed 64bits native	3 / 63	2018-07-02 13:00:42	2018-07-02 13:00:42	1	1	12.8 KB
□	85eb616ab4424ea27ea3dcad7df1a8b7a5ed8e533212927e2b1dfb03679c758f e71a3adbe7eb8aed5fe7c97f8451eb2c peexe assembly overlay signed 64bits native	5 / 64	2018-07-02 08:53:10	2018-07-02 08:53:10	1	1	16.6 KB
□	50bf5b7626970f5213cacf595b1f442b7538665228e768c13c2feb2b0485b919 f5bedb5bd7534608ca4958a8b0f82bcd peexe assembly overlay revoked-cert signed 64bits native	33 / 63	2018-07-02 00:56:20	2018-07-02 00:56:20	1	1	113.8 KB
□	4a7e58331d7765a12f53dc2371739dc9a463940b13e16157ce10db80e958d740 548260a7b8654e024dc30bf8a7c5baa4	0 / 64	2010-02-11 15:38:47	2018-07-01 19:20:27	349	45	91.0 KB

HACKING

SECURITY

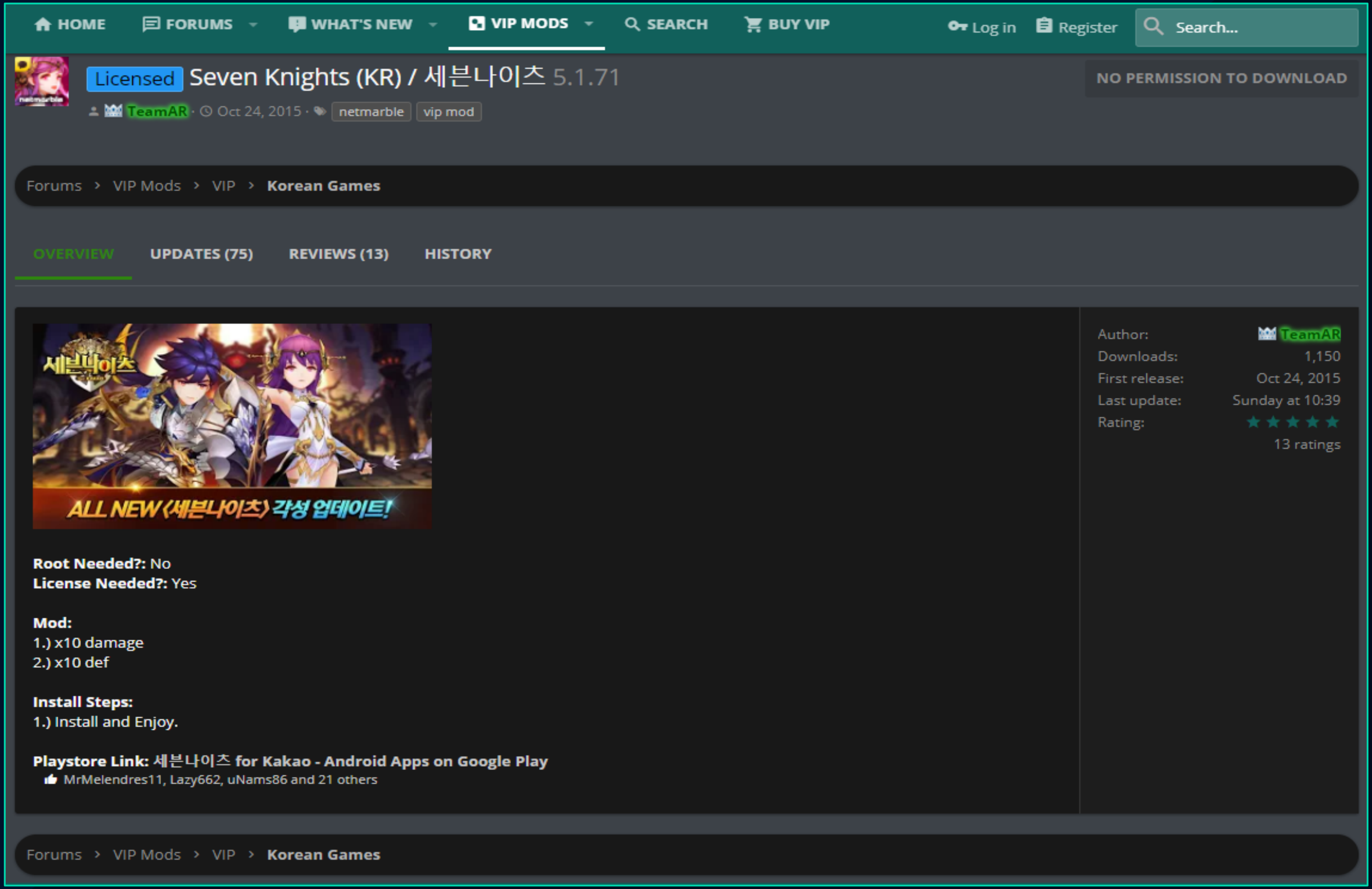
XIGNCODE3
Copyright(C) 2015 Wellbia.com Co., Ltd
All rights reserved

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

X·TRAP
X-TRAP Web Management System

INCA
Internet
nProtect GameGuard
No.1 Global Game Security Solution

MOBILE



Licensed Seven Knights (KR) / 세븐나이츠 5.1.71

TeamAR · Oct 24, 2015 · netmarble vip mod

Forums › VIP Mods › VIP › **Korean Games**

OVERVIEW UPDATES (75) REVIEWS (13) HISTORY

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**

HACKING

끝으로...

Q&A