
GameHack,

오토샷부터 월핵까지

넥슨GT 서든어택1실 서미혜

Who am I?

여자
사람
분석가

WARNING

경고

본 발표의 내용을 토대로 특정 게임의 핵(불법 프로그램)을
제작or유포or판매할 경우 ·민형사상의 처벌이 있음을 알려드립니다.
또한, 계정 영구 정지와 같은 게임상의 불이익을 받을 수 있으며,
이후 생성하는 모든 계정이 차단될 수 있음을 알려 드립니다.

Contents

1. GameHack 종류
2. GameHack 동작 방식
3. Demo
4. Q/A



1. GameHack 종류

멀웨어



1. GameHack 종류

무반+에임고정



1. GameHack 종류

레이더핵



1. GameHack 종류

레이더해킹



1. GameHack 종류

레이더핵



1. GameHack 종류

오토에임



1. GameHack 종류

여기까지만 ?

1. GameHack 종류

매크로
라운드 종료
방월
고텔
벽뚫
병월
스왑장전
Chams
관통
무기고 인피니티
오토텔
자유시점
제패
오토샷
데스노트
내변
도배무시
인피니티
형광 캐릭터
헤드고정
모션
유체이탈
즉리
공백닉
무적
외변
총알무한
오토에임
누킹
ESP



2. GameHack 동작방식

외부 or 내부

2. GameHack 동작방식

외부 or 내부

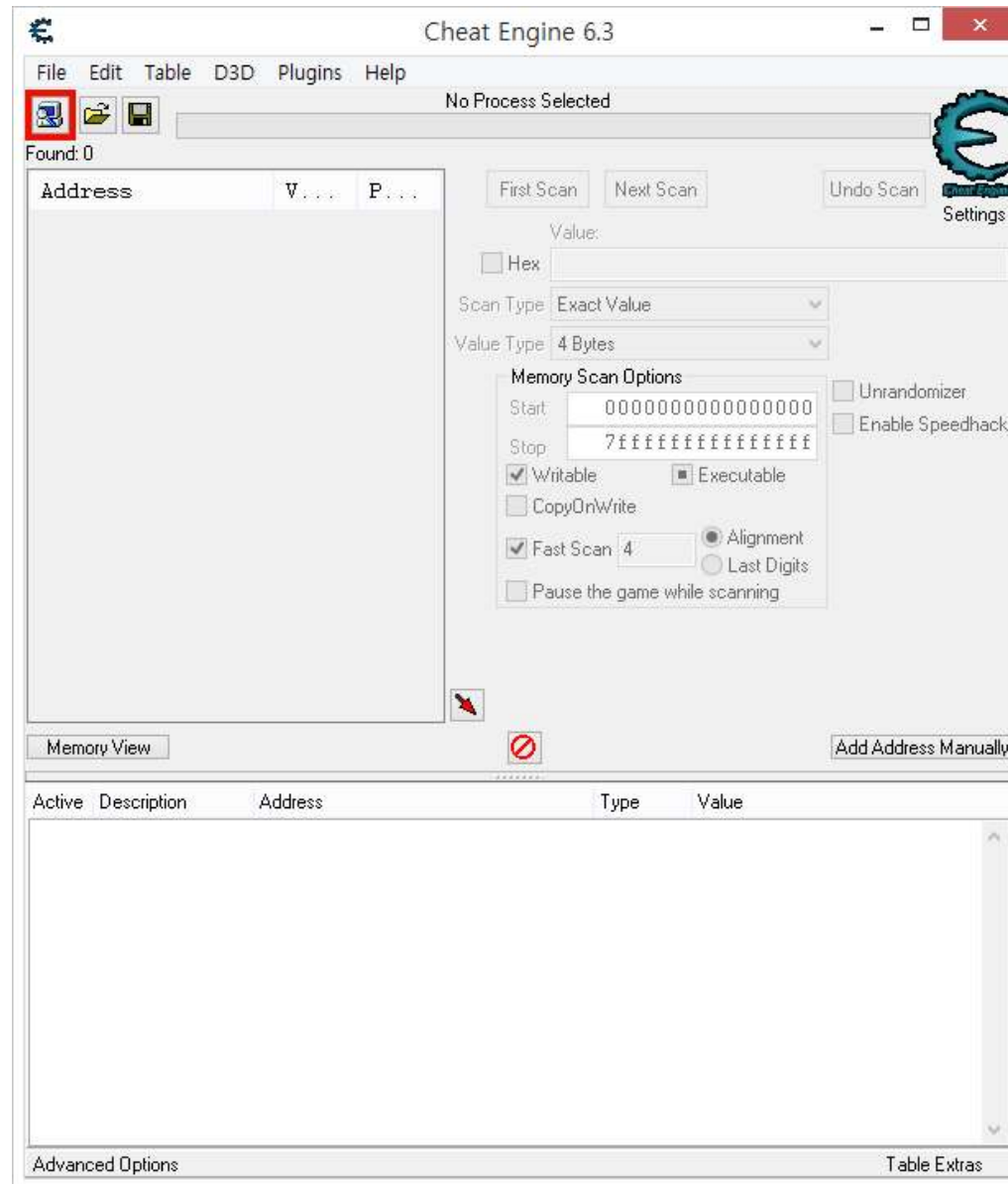
2. GameHack 동작방식 - 외부

EXE

2. GameHack 동작방식 - 외부



Hacker



Defender

2. GameHack 동작방식

외부 or 내부

2. GameHack 동작방식 - 내부

INJECTION

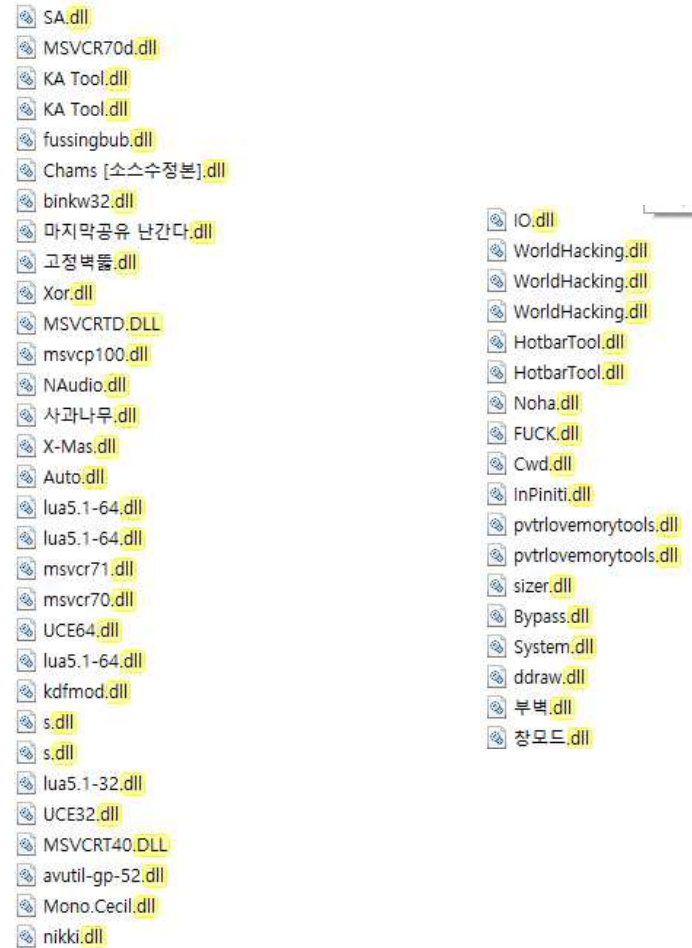
2. GameHack 동작방식 - 내부

DLL or CODE

2. GameHack 동작방식 - 내부

DLL or CODE

2. GameHack 동작방식 – 내부(DLL)



2. GameHack 동작방식(클라이언트 내부동작-DLL)

The screenshot displays a debugger window with the 'Modules' tab selected. The 'SampleHack.dll' module is highlighted in the list. An arrow points from this module to the assembly view on the right. The assembly view shows the following instructions:

Address	Disassembly
SampleHack.dfprintf+72	8B F4 mov esi,esp
SampleHack.dfprintf+74	68 00470630 push SampleHack.dll+64700 [002B2B61]
SampleHack.dfprintf+79	8B 45 08 mov eax,[ebp+08]
SampleHack.dfprintf+7C	50 push eax
SampleHack.dfprintf+7D	FF 15 4C0B0930 call dword ptr [SampleHack._imp__fopen] ->MSVCR71D.fopen
SampleHack.dfprintf+83	83 C4 08 add esp,08
SampleHack.dfprintf+86	3B F4 cmp esi,esp
SampleHack.dfprintf+88	E8 9473FFFF call SampleHack.dll+20AE1
SampleHack.dfprintf+8D	89 85 E0FEFFFF mov [ebp-00000120],eax
SampleHack.dfprintf+93	8B F4 mov esi,esp
SampleHack.dfprintf+95	8D 85 F8FEFFFF lea eax,[ebp-00000108]
SampleHack.dfprintf+9B	50 push eax
SampleHack.dfprintf+9C	68 70460630 push SampleHack.dll+64670 [00007325]
SampleHack.dfprintf+A1	8B 8D E0FEFFFF mov ecx,[ebp-00000120]
SampleHack.dfprintf+A7	51 push ecx
SampleHack.dfprintf+A8	FF 15 500B0930 call dword ptr [SampleHack._imp__fprintf] ->MSVCR71D.fprintf
SampleHack.dfprintf+AE	83 C4 0C add esp,0C
SampleHack.dfprintf+B1	3B F4 cmp esi,esp
SampleHack.dfprintf+B3	E8 6973FFFF call SampleHack.dll+20AE1
SampleHack.dfprintf+B8	8B F4 mov esi,esp
SampleHack.dfprintf+BA	8D 85 F8FEFFFF lea eax,[ebp-00000108]
SampleHack.dfprintf+C0	50 push eax
SampleHack.dfprintf+C1	FF 15 000B0930 call dword ptr [SampleHack._imp__OutputDebugStringA] ->KERNELBASE.OutputDebugStringA
SampleHack.dfprintf+C7	3B F4 cmp esi,esp
SampleHack.dfprintf+C9	E8 5373FFFF call SampleHack.dll+20AE1
SampleHack.dfprintf+CE	52 push edx
SampleHack.dfprintf+CF	8B CD mov ecx,ebp

2. GameHack 동작방식 - 내부

DLL or CODE

2. GameHack 동작방식 - 내부(CODE)

The screenshot displays the Immunity Debugger interface with the 'Strings' window open for the process 'suddenattack.exe (8204)'. The 'Strings' window shows a list of memory addresses and their corresponding string data. A specific string is highlighted, and an arrow points from it to a hex editor window. The hex editor window shows the raw bytes of the selected string, along with buttons for 'Re-read', 'Write', 'Goto...', 'Save...', and 'Close'.

Name	Address	Size	Protect...
Free	0xe341000	60 kB	NA
Private (Commit)	0xe350000	4 kB	RW
Free	0xe351000	60 kB	NA
Private (Commit)	0xe360000	4 kB	RW
Free	0xe361000	60 kB	NA
Private (Commit)	0xe370000	4 kB	RW
Free	0xe371000	60 kB	NA
Private (Commit)	0xe380000	4 kB	RW
Free	0xe381000	60 kB	NA
Private (Commit)	0xe390000	4 kB	RW
Free	0xe391000	60 kB	NA
Private (Commit)	0xe3a0000	4 kB	RW
Free	0xe3a1000	60 kB	NA
Private (Commit)	0xe3b0000	4 kB	RWX
Free	0xe3b1000	60 kB	NA
Private (Commit)	0xe3c0000	4 kB	RWX
Free	0xe3c1000	60 kB	NA
Private (Commit)	0xe3d0000	4 kB	RWX
Free	0xe3d1000	60 kB	NA
Mapped (Commit)	0xe3e0000	4 kB	RW
Free	0xe3e1000	60 kB	NA
Private (Reserve)	0xe3f0000	212 kB	
Private (Commit)	0xe425000	12 kB	RW+G
Private (Commit)	0xe428000	32 kB	RW
Private (Reserve)	0xe430000	1,012 kB	
Private (Commit)	0xe52d000	8 kB	RW+G

The hex editor window shows the following data:

```

00000000 55 8b ec 83 ec 40 53 56 57 b8 01 00 00 00 85 c0 U...@SVW.....
00000010 74 18 68 e9 03 00 00 ff 15 00 00 3d 0e 68 00 00 t.h.....=.h..
00000020 3c 0e ff 15 04 00 3d 0e eb df 5f 5e 5b 8b e5 5d <.....=...^[...]
00000030 c3 cc 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
  
```


2. GameHack 동작방식

끝?

2. GameHack 동작방식 – 그 외

리소스 변경

2. GameHack 동작방식 – 그 외(리소스)

외변



2. GameHack 동작방식 – 그 외(리소스)

외변



2. GameHack 동작방식 – 그 외(리소스)

내변



2. GameHack 동작방식 – 그 외(리소스)

형광 캐릭터



3. Demo

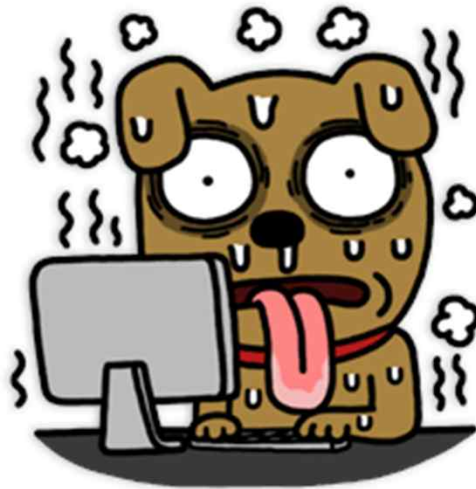


WE ALWAYS KEEP
WATCHING U

4. Q&A



Q&A



Thank you