ANTI-CHEAT FOR MULTIPLAYER GAMES

Simon Allaeys, Aarni Rautava

Who we are

2006

Hobby project

Third-party CS anti-cheat

2013 - Today

25+ online multiplayer games worldwide

Team of 14 based in Helsinki, Finland

Actively researching the domain

EASYANTICHEAT
DON'T BEAR WITH THE CHEATERS

Questions Answered

What is cheating?

Who is doing it?

How is it done?

Anti-cheating?

CHEATING

(╯°□°）╯︵ ┻━┻

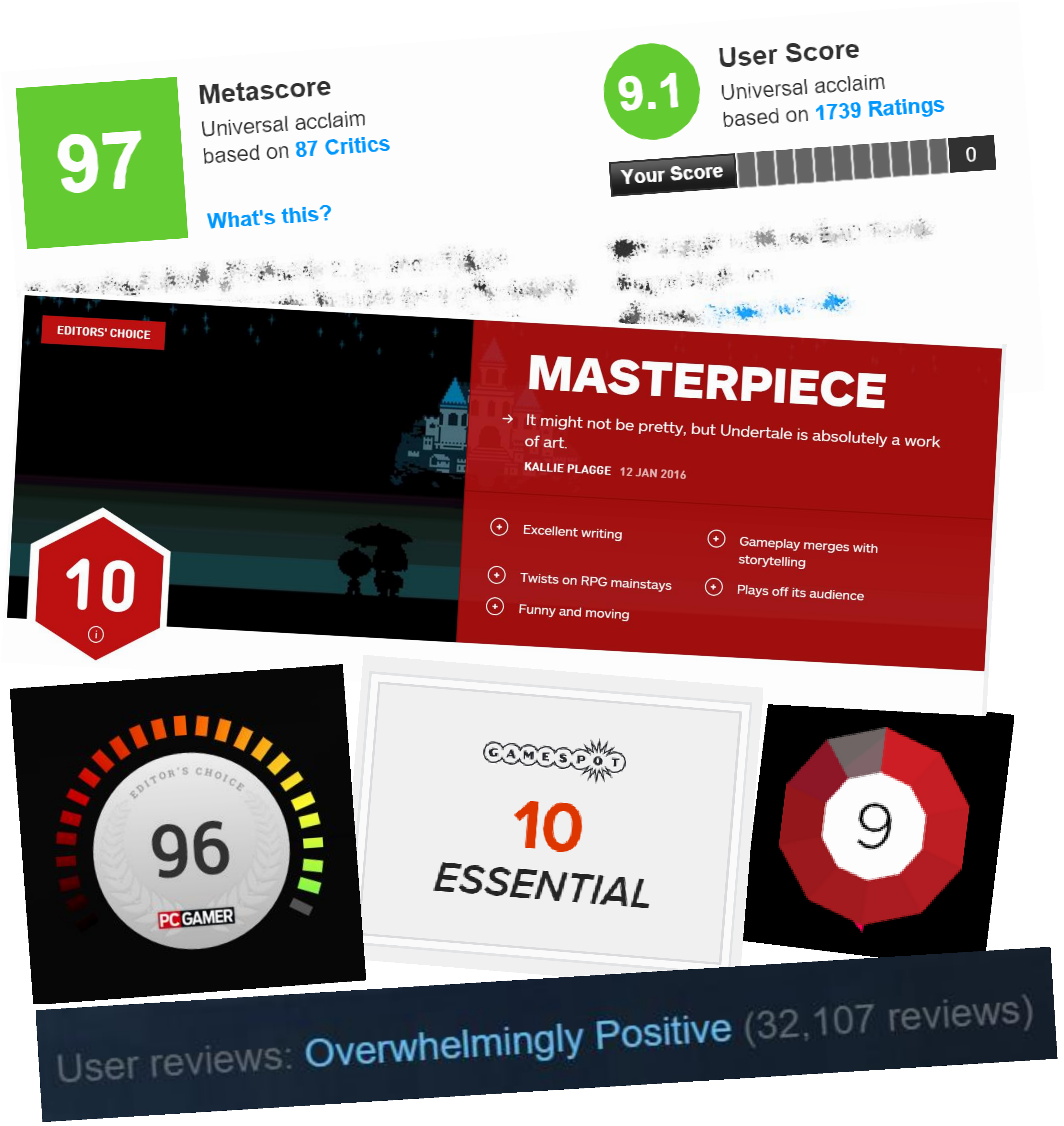
Cheating?

Gaining an
unfair advantage

Cheating?

G1
G2
G3
Esc
G4
G5
G6
G7
G8
G9
G10
G11
G12
G13
G14
G15
G16
G17
G18
Ctr
[69]OSC
[57]Entropy
[42]Monarch
(44M) BLAIN IS AIMING AT YOU
[96]Cathode
(48m)

Exploits Automation Overlays State Manipulation



97

Metascore

Universal acclaim

based on 87 Critics

What's this?

9.1

User Score

Universal acclaim

based on 1739 Ratings

Your Score 0

EDITORS' CHOICE

10

MASTERPIECE

It might not be pretty, but Undertale is absolutely a work of art.

KALLIE PLAGGE 12 JAN 2016

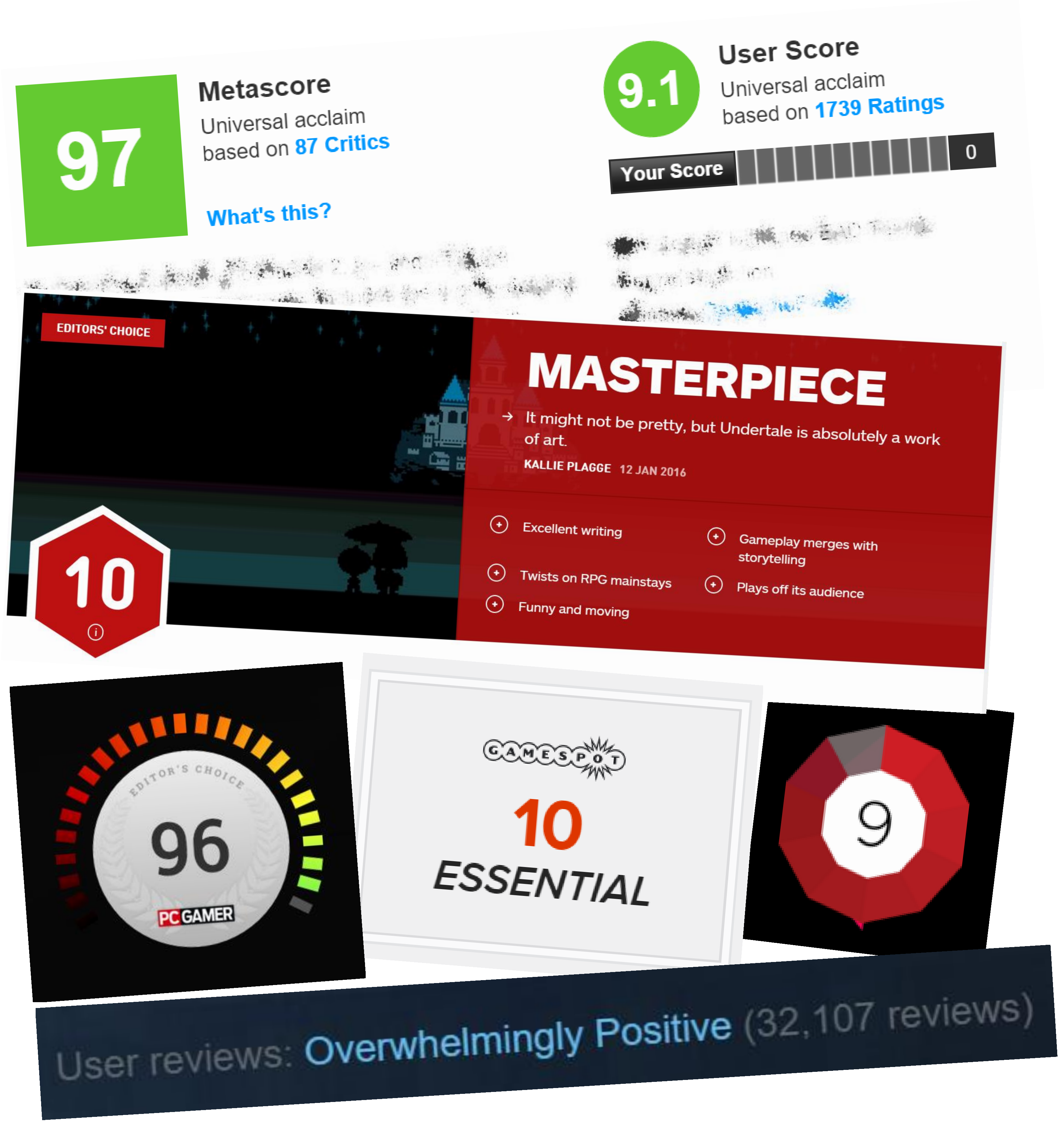
- Excellent writing
- Gameplay merges with storytelling
- Twists on RPG mainstays
- Plays off its audience
- Funny and moving

EDITOR'S CHOICE 96 PC GAMER

GAMESPOT 10 ESSENTIAL

9

User reviews: Overwhelmingly Positive (32,107 reviews)


97 Metascore
Universal acclaim
based on 87 Critics

What's this?

9.1 User Score
Universal acclaim
based on 1739 Ratings

Your Score 0

EDITORS' CHOICE

10

MASTERPIECE

→ It might not be pretty, but Undertale is absolutely a work of art.

KALLIE PLAGGE 12 JAN 2016

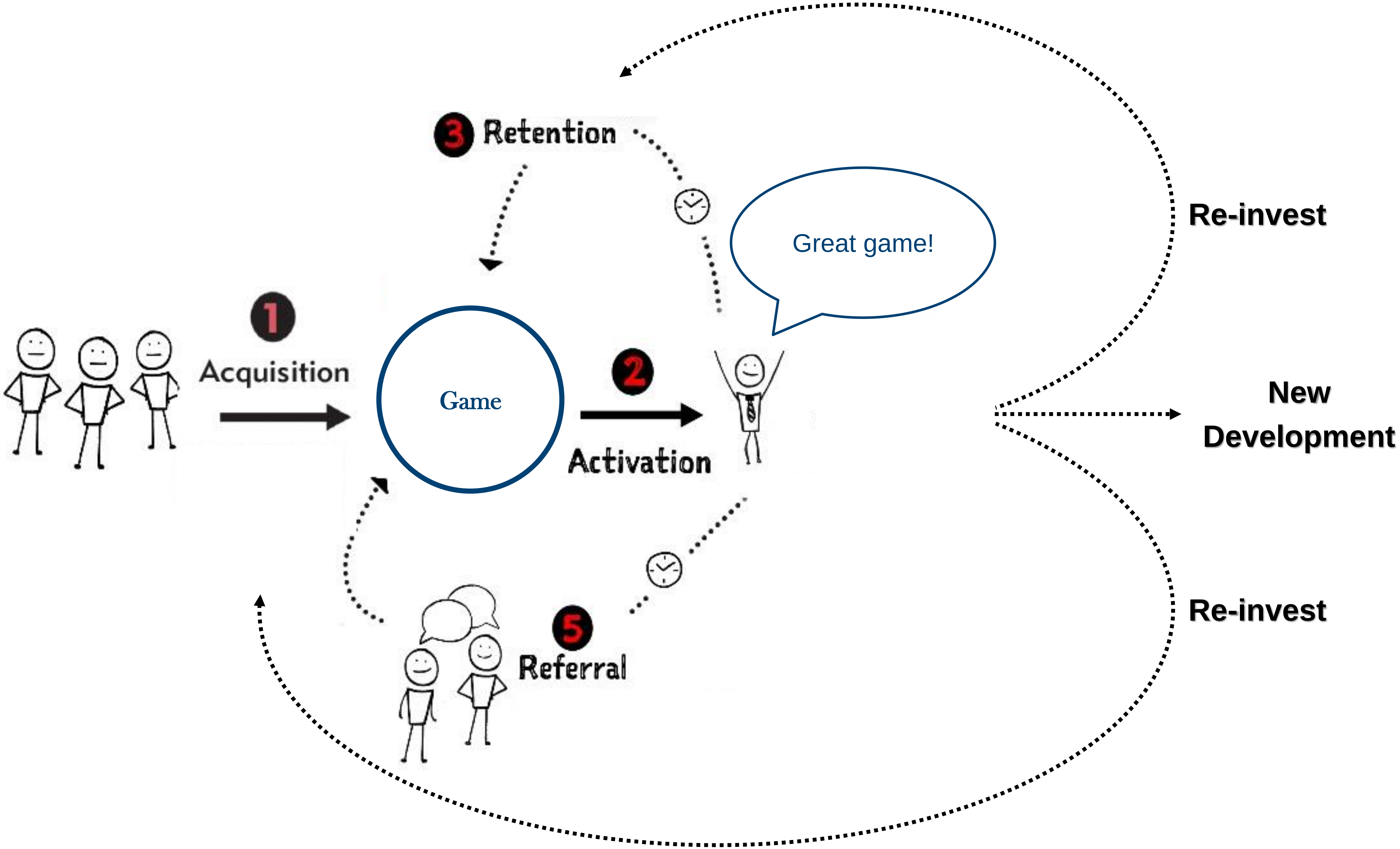
- Excellent writing
- Gameplay merges with storytelling
- Twists on RPG mainstays
- Plays off its audience
- Funny and moving

EDITOR'S CHOICE 96 PC GAMER

GAMESPOT 10 ESSENTIAL

9

User reviews: Overwhelmingly Positive (32,107 reviews)



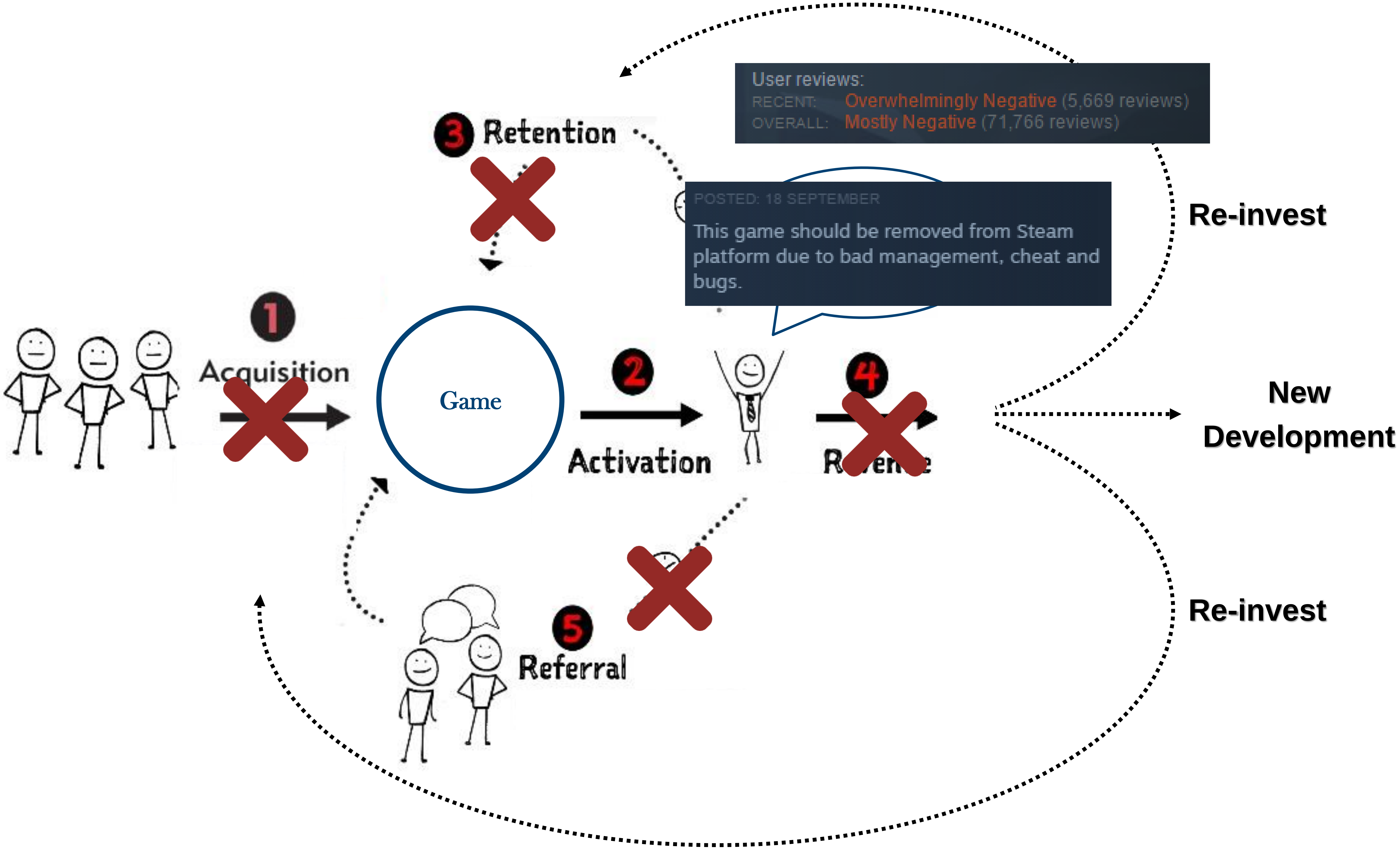
Game

Great game!

Re-invest

New Development

Re-invest



User reviews:

RECENT: Overwhelmingly Negative (5,669 reviews)

OVERALL: Mostly Negative (71,766 reviews)

POSTED: 18 SEPTEMBER

This game should be removed from Steam platform due to bad management, cheat and bugs.

Re-invest

New Development

Re-invest

CHEATERS

(╯°□°) ╯︵(\ .O.)\

Some definitions

Who are they?

HACKERS → PROVIDERS → CHEATERS

HACKERS

- R&D
- Loader/Injector
- Features
- DRM

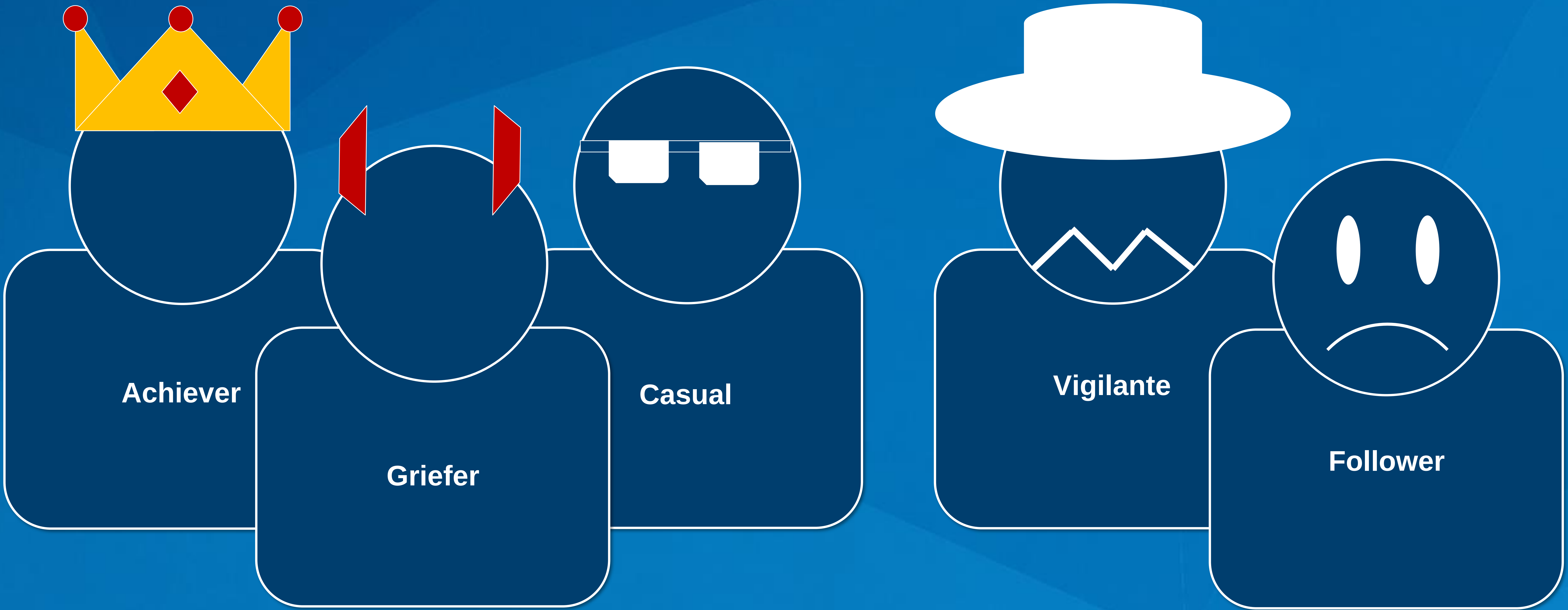
PROVIDERS

- Branding
- Community
- Payments
- Localization

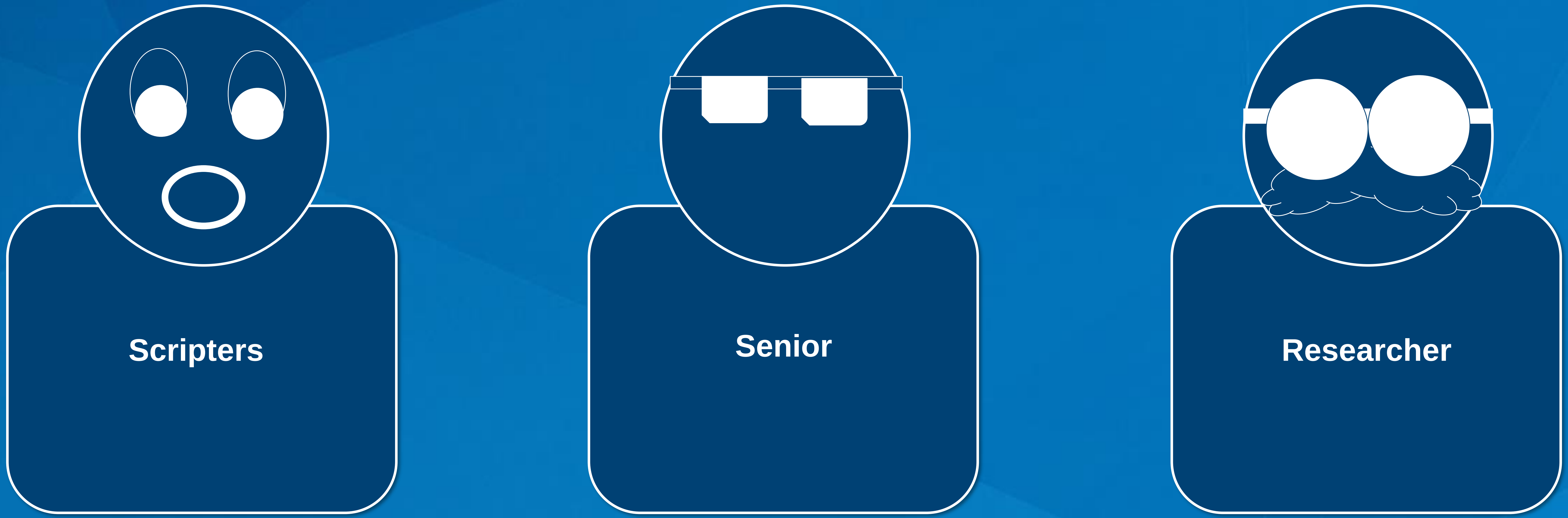
CHEATERS

- Players / Users

HACKERS → PROVIDERS → CHEATERS



HACKERS → PROVIDERS → CHEATERS



Scripters

Senior

Researcher

HACKERS → PROVIDERS → CHEATERS

Open Communities

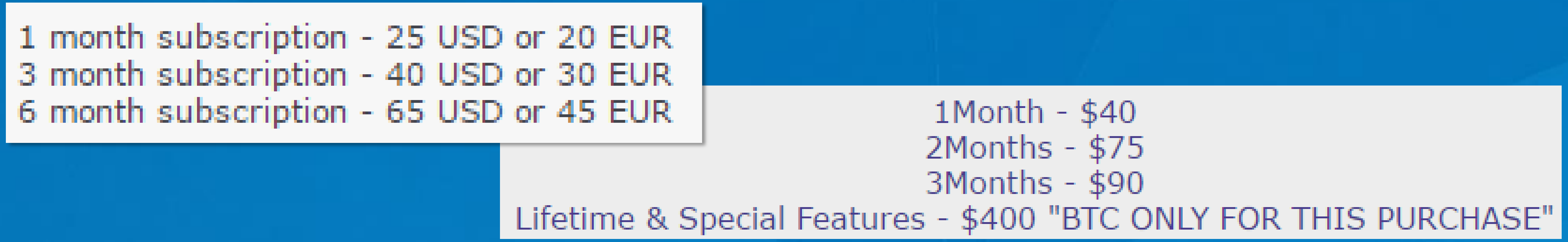
- ✓ Free cheats
- ✓ Easy access
- ✓ Knowledge sharing

Cheat Publishers

- ✓ Paid cheats
- ✓ Easy access

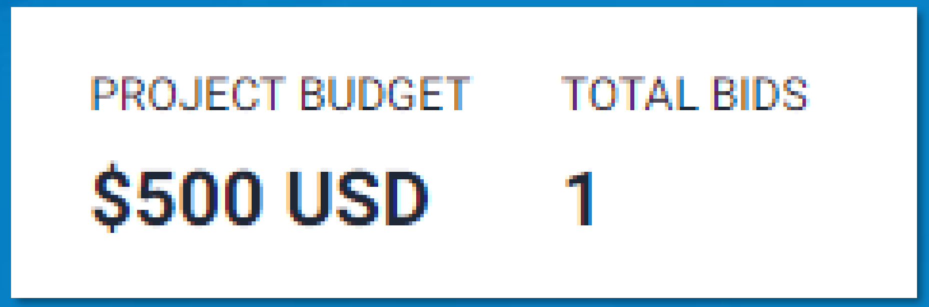
Closed Communities

- ✓ Private cheats
- ✓ Reputation based access
- ✓ Limited availability



1 month subscription - 25 USD or 20 EUR
3 month subscription - 40 USD or 30 EUR
6 month subscription - 65 USD or 45 EUR

1Month - $40
2Months - $75
3Months - $90
Lifetime & Special Features - $400 "BTC ONLY FOR THIS PURCHASE"



PROJECT BUDGET	TOTAL BIDS
$500 USD	1

It’s a business

Cheating as an industry

Free public cheats

Public commercial cheats

Paid private cheats

Private exclusive cheats

Legitimate businesses

- ✓ Registered companies
- ✓ Tax payments
- ✓ Professional management

One Person Company

… - $750k a year - …

Teams

… - $1.5M a year - …

Global market size?

> $100M

CHEATS

ლ(▀̿Ĺ̯▀̿ ̿ლ)

Exploits and scripts

Everyone has done it

In-game glitching

Console variables and game options

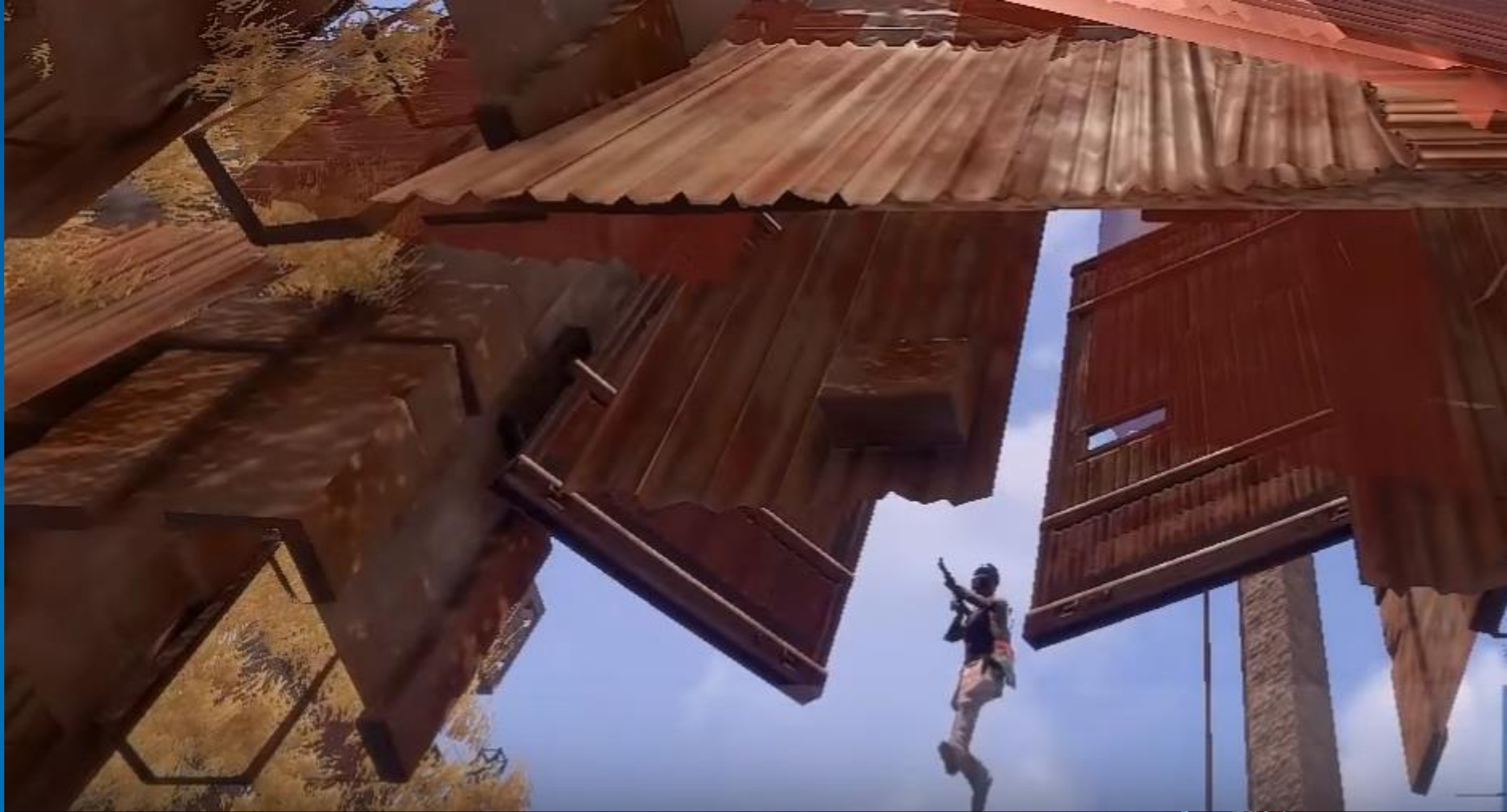
Game debug console

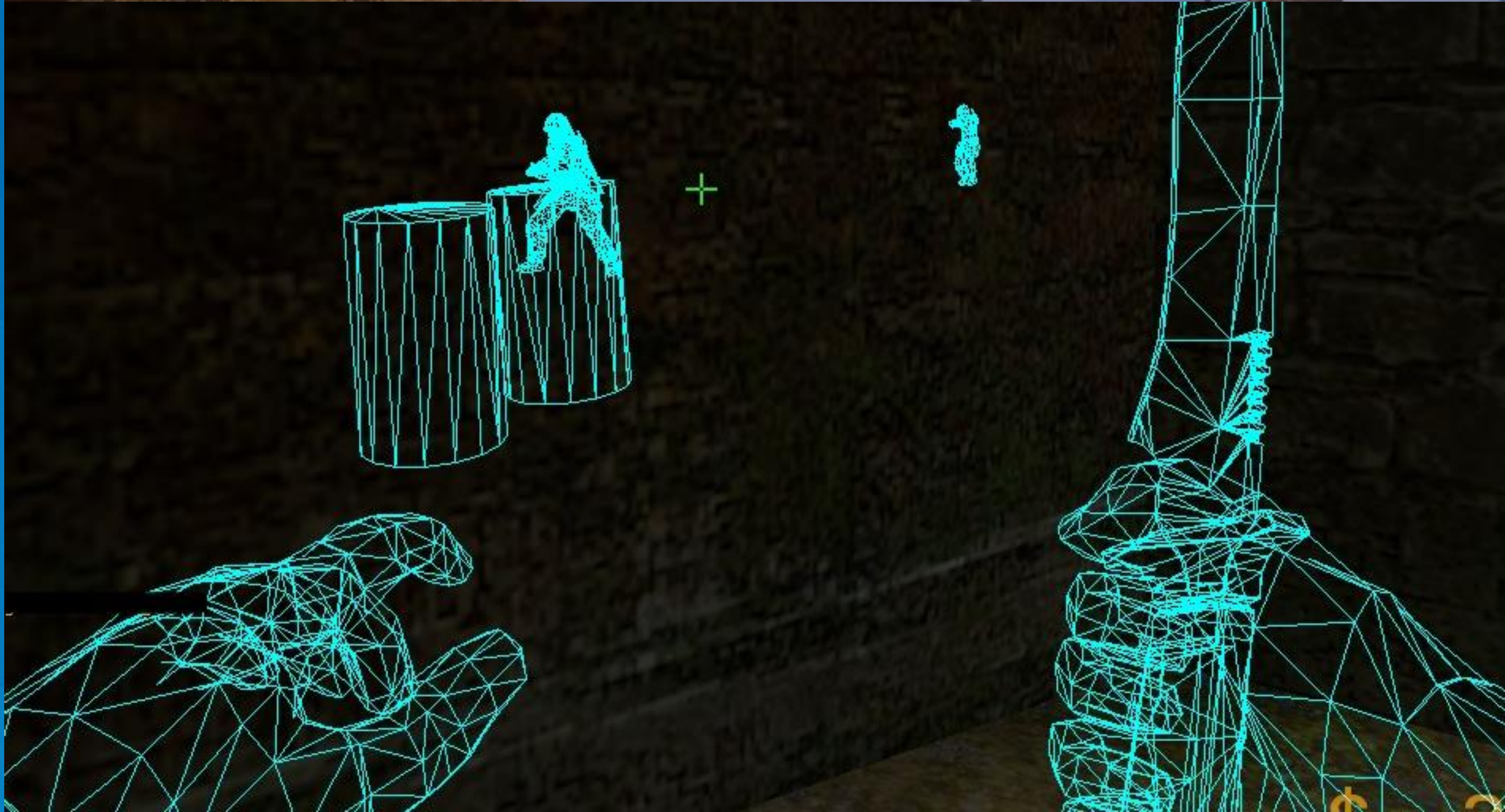
File modding

→ Enforce valid variable values

→ Exclude debug options from releases

→ Check game files integrity





..downloaded a tool

Game manipulation

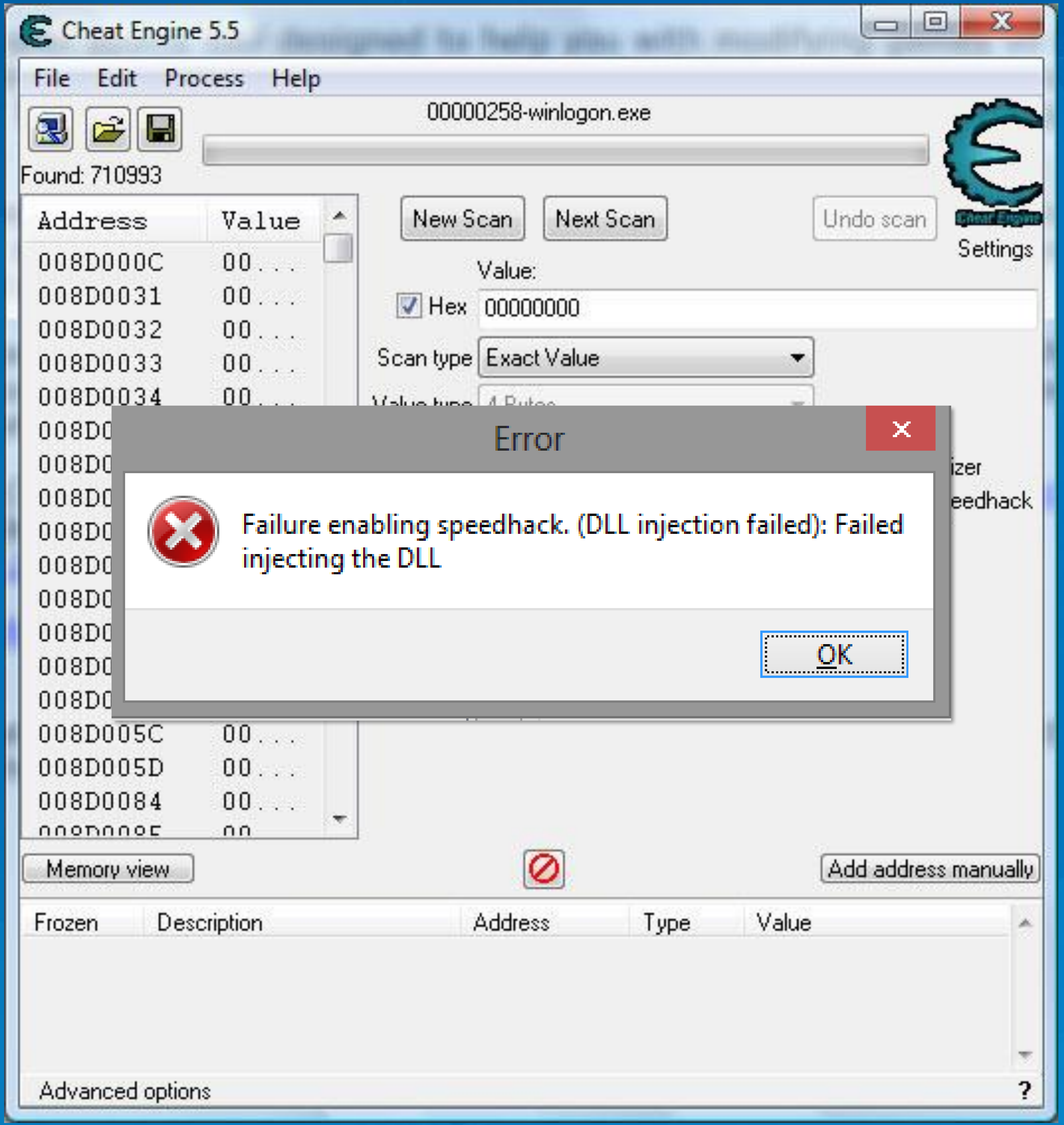
Poking around..

Game state manipulation

→ Authoritative game servers

→ Obfuscation and encryption

→ Anti-cheat prevention or detection



00000258-winlogon.exe

Found: 710993

```
Address    Value
008D000C   00...
008D0031   00...
008D0032   00...
008D0033   00...
008D0034   00...
008D005C   00...
008D005D   00...
008D0084   00...
```

Value:

☑ Hex 00000000

Scan type Exact Value

Failure enabling speedhack. (DLL injection failed): Failed injecting the DLL

Frozen	Description	Address	Type	Value

Cheat v0.1

Writing your own cheat

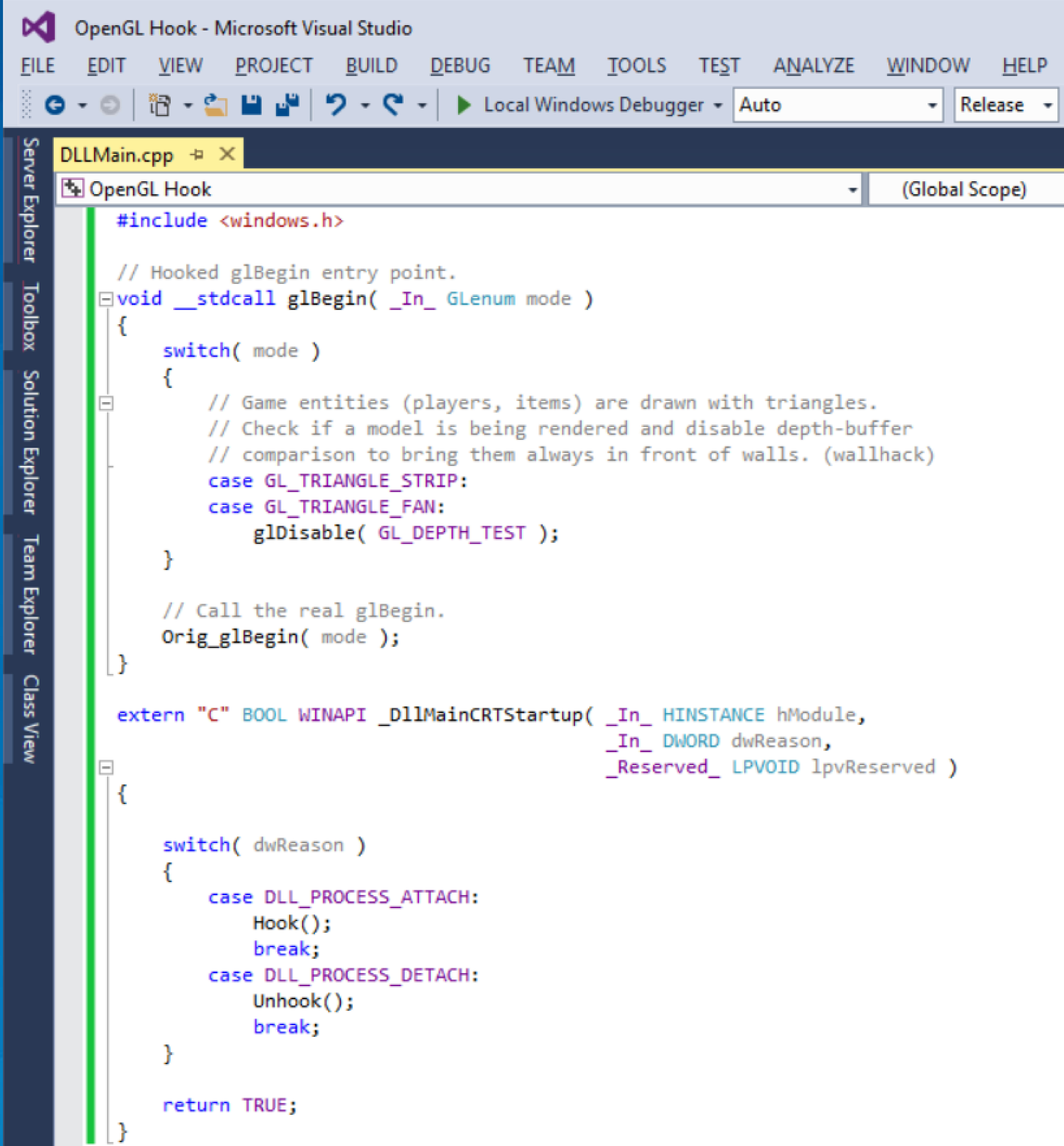
Open source cheat examples

Documented game engine dependencies

- Hijack dependencies

Documented game engine interfaces

- Hack as a plugin



```
#include <windows.h>

// Hooked glBegin entry point.
void __stdcall glBegin( _In_ GLenum mode )
{
    switch( mode )
    {
        // Game entities (players, items) are drawn with triangles.
        // Check if a model is being rendered and disable depth-buffer
        // comparison to bring them always in front of walls. (wallhack)
        case GL_TRIANGLE_STRIP:
        case GL_TRIANGLE_FAN:
            glDisable( GL_DEPTH_TEST );
    }

    // Call the real glBegin.
    Orig_glBegin( mode );
}

extern "C" BOOL WINAPI _DllMainCRTStartup( _In_ HINSTANCE hModule,
                                           _In_ DWORD dwReason,
                                           _Reserved_ LPVOID lpvReserved )
{

    switch( dwReason )
    {
        case DLL_PROCESS_ATTACH:
            Hook();
            break;
        case DLL_PROCESS_DETACH:
            Unhook();
            break;
    }

    return TRUE;
}
```

Cheat v0.1

Writing your own cheat

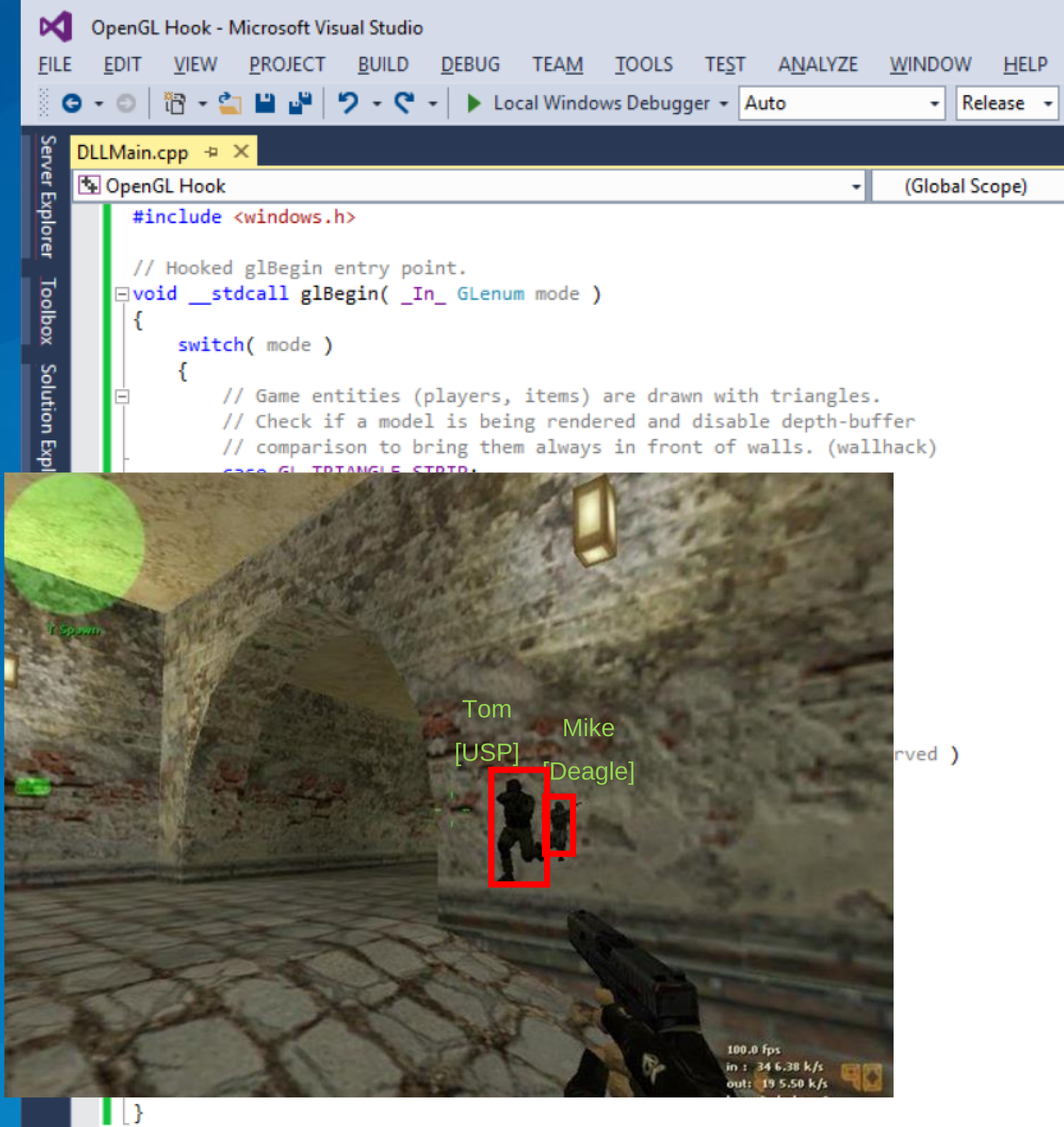
Open source cheat examples

Documented game engine dependencies

- Hijack dependencies

Documented game engine interfaces

- Hack as a plugin



```
#include <windows.h>

// Hooked glBegin entry point.
void __stdcall glBegin( _In_ GLenum mode )
{
    switch( mode )
    {
        // Game entities (players, items) are drawn with triangles.
        // Check if a model is being rendered and disable depth-buffer
        // comparison to bring them always in front of walls. (wallhack)
        case GL_TRIANGLE_STRIP:
```

```
rved )
```

```
}
```

Bot v0.1

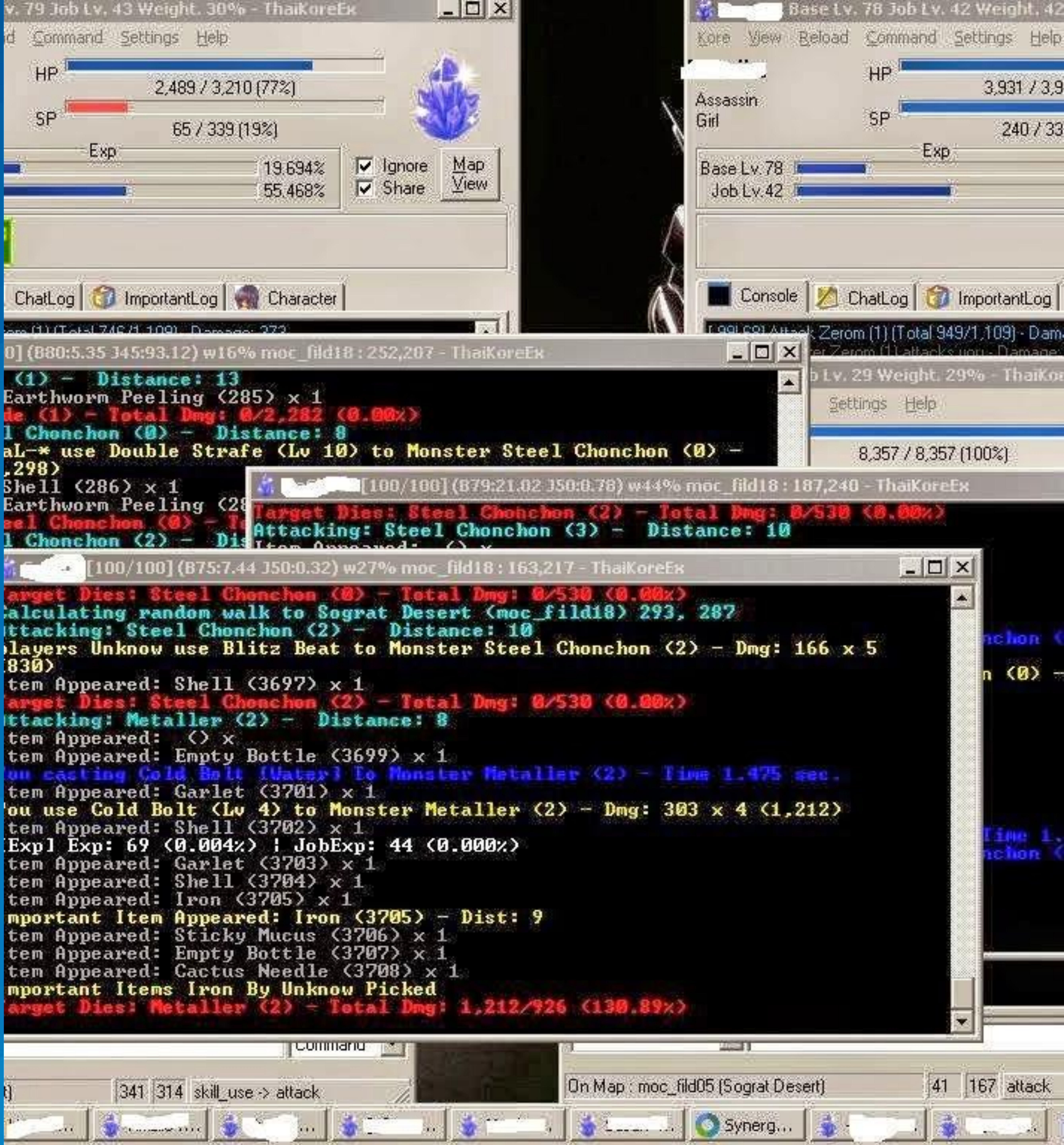
Writing your own bot

Open source bot examples

Automated player input

Plain text protocol?

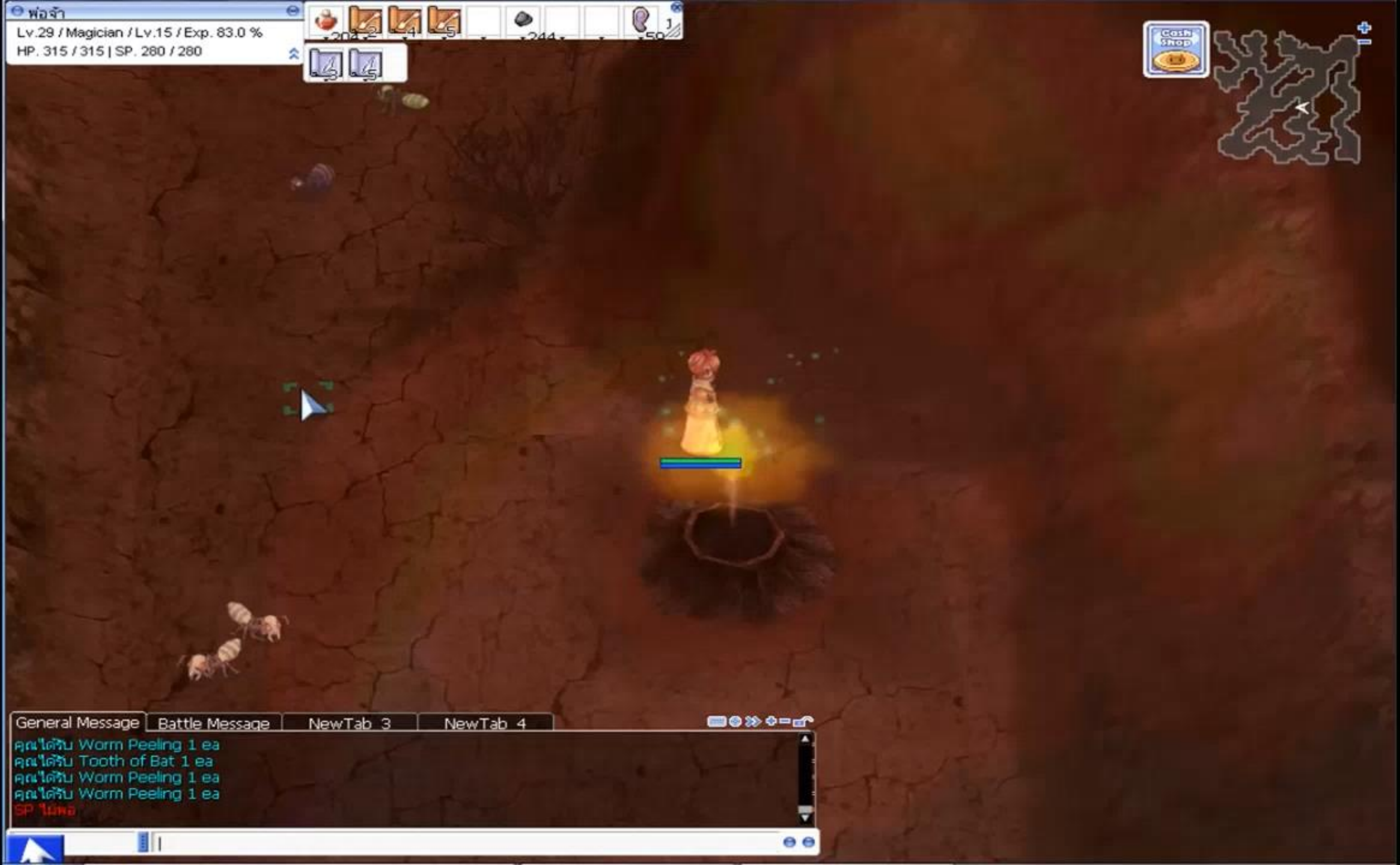
Farm, farm, farm.... profit!



```
0] (880:5.35 345:93.12) w16% moc_fild18 : 252,207 - ThaiKoreEx
 (1) -  Distance: 13
Earthworm Peeling (285) x 1
de (1) - Total Dmg: 0/2,282 (0.00%)
l Chonchon (0) -  Distance: 8
aL-* use Double Strafe (Lv 10) to Monster Steel Chonchon (0) -
,298)
Shell (286) x 1
Earthworm Peeling (28
eel Chonchon (0) - T
l Chonchon (2) -  Dis
```

```
[redacted] [100/100] (879:21.02 350:8.78) w44% moc_fild18 : 187,240 - ThaiKoreEx
Target Dies: Steel Chonchon (2) - Total Dmg: 0/530 (0.00%)
Attacking: Steel Chonchon (3) -  Distance: 10
```

```
[redacted] [100/100] (875:7.44 350:0.32) w27% moc_fild18 : 163,217 - ThaiKoreEx
arget Dies: Steel Chonchon (0) - Total Dmg: 0/530 (0.00%)
alculating random walk to Sograt Desert (moc_fild18) 293, 287
ttacking: Steel Chonchon (2) -  Distance: 10
layers Unknow use Blitz Beat to Monster Steel Chonchon (2) - Dmg: 166 x 5
830)
tem Appeared: Shell (3697) x 1
arget Dies: Steel Chonchon (2) - Total Dmg: 0/530 (0.00%)
ttacking: Metaller (2) -  Distance: 8
tem Appeared:  () x
tem Appeared: Empty Bottle (3699) x 1
ou casting Cold Bolt [Water] To Monster Metaller (2) - Time 1.475 sec.
tem Appeared: Garlet (3701) x 1
ou use Cold Bolt (Lv 4) to Monster Metaller (2) - Dmg: 303 x 4 (1,212)
tem Appeared: Shell (3702) x 1
Exp] Exp: 69 (0.004%) ¦ JobExp: 44 (0.000%)
tem Appeared: Garlet (3703) x 1
tem Appeared: Shell (3704) x 1
tem Appeared: Iron (3705) x 1
mportant Item Appeared: Iron (3705) - Dist: 9
tem Appeared: Sticky Mucus (3706) x 1
tem Appeared: Empty Bottle (3707) x 1
tem Appeared: Cactus Needle (3708) x 1
mportant Items Iron By Unknow Picked
arget Dies: Metaller (2) - Total Dmg: 1,212/926 (130.89%)
```



Lv.29 / Magician / Lv.15 / Exp. 83.0 %
HP. 315 / 315 | SP. 280 / 280

คุณได้รับ Worm Peeling 1 ea
คุณได้รับ Tooth of Bat 1 ea
คุณได้รับ Worm Peeling 1 ea
คุณได้รับ Worm Peeling 1 ea
SP ไม่พอ

Cheat v1.0

Feature rich cheats

<u>Inject Cheat Features</u>

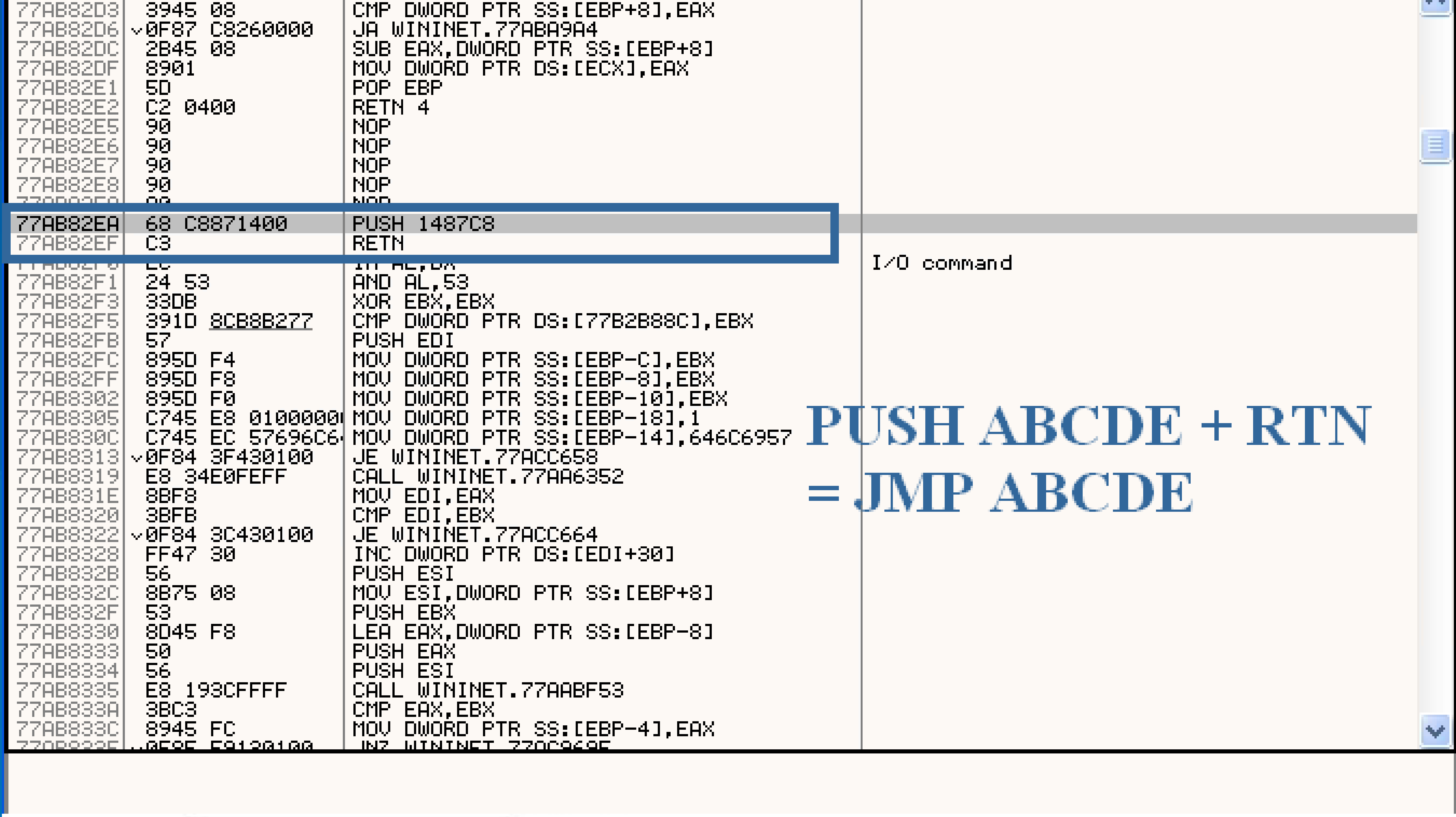
Inline code patches

Interface pointer hooks

Hijacking exception handling

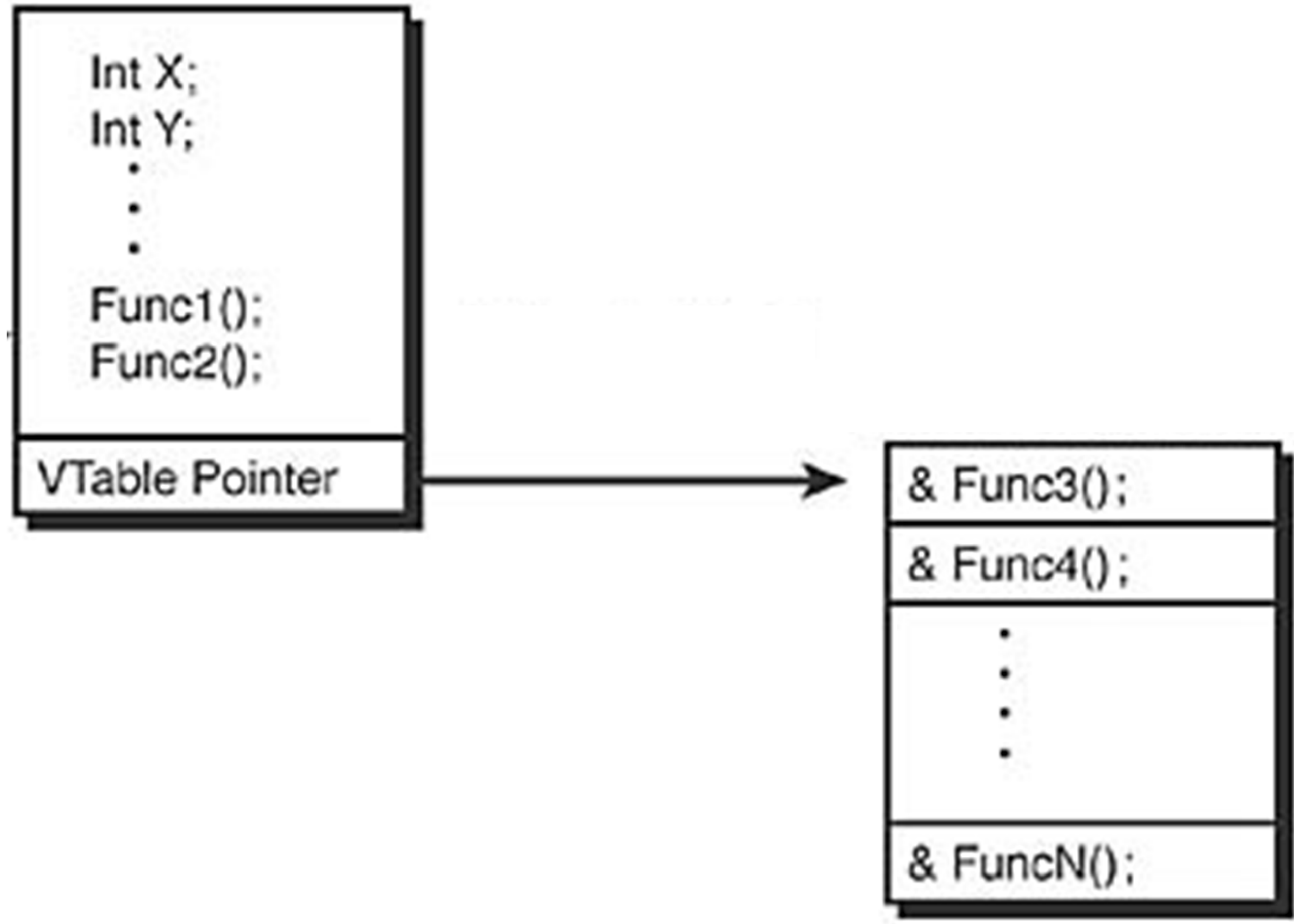
Hardware debug breakpoints

…



```
77AB82D3   3945 08         CMP DWORD PTR SS:[EBP+8],EAX
77AB82D6  v0F87 C8260000   JA WININET.77ABA9A4
77AB82DC   2B45 08         SUB EAX,DWORD PTR SS:[EBP+8]
77AB82DF   8901            MOV DWORD PTR DS:[ECX],EAX
77AB82E1   5D              POP EBP
77AB82E2   C2 0400         RETN 4
77AB82E5   90              NOP
77AB82E6   90              NOP
77AB82E7   90              NOP
77AB82E8   90              NOP
77AB82EA   68 C8871400     PUSH 1487C8
77AB82EF   C3              RETN
77AB82F0   EC              IN AL,DX                        I/O command
77AB82F1   24 53           AND AL,53
77AB82F3   33DB            XOR EBX,EBX
77AB82F5   391D 8CB8B277   CMP DWORD PTR DS:[77B2B88C],EBX
77AB82FB   57              PUSH EDI
77AB82FC   895D F4         MOV DWORD PTR SS:[EBP-C],EBX
77AB82FF   895D F8         MOV DWORD PTR SS:[EBP-8],EBX
77AB8302   895D F0         MOV DWORD PTR SS:[EBP-10],EBX
77AB8305   C745 E8 0100000 MOV DWORD PTR SS:[EBP-18],1
77AB830C   C745 EC 57696C6 MOV DWORD PTR SS:[EBP-14],646C6957
77AB8313  v0F84 3F430100   JE WININET.77ACC658
77AB8319   E8 34E0FEFF     CALL WININET.77AA6352
77AB831E   8BF8            MOV EDI,EAX
77AB8320   3BFB            CMP EDI,EBX
77AB8322  v0F84 3C430100   JE WININET.77ACC664
77AB8328   FF47 30         INC DWORD PTR DS:[EDI+30]
77AB832B   56              PUSH ESI
77AB832C   8B75 08         MOV ESI,DWORD PTR SS:[EBP+8]
77AB832F   53              PUSH EBX
77AB8330   8D45 F8         LEA EAX,DWORD PTR SS:[EBP-8]
77AB8333   50              PUSH EAX
77AB8334   56              PUSH ESI
77AB8335   E8 193CFFFF     CALL WININET.77AABF53
77AB833A   3BC3            CMP EAX,EBX
77AB833C   8945 FC         MOV DWORD PTR SS:[EBP-4],EAX
```

PUSH ABCDE + RTN
= JMP ABCDE



Cheat v1.0

Feature rich cheats

Inject Cheat Features

Inline code patches

Interface pointer hooks

Hijacking exception handling

Hardware debug breakpoints

…

Protect the cheat itself

DKOM (Hiding processes, drivers, ..)

Interrupt hooks

System service hooks (NTAPI)

VAD hiding (Hiding cheat memory)

…

DRM, hardware locking, monitor usage

Cheat v4.0

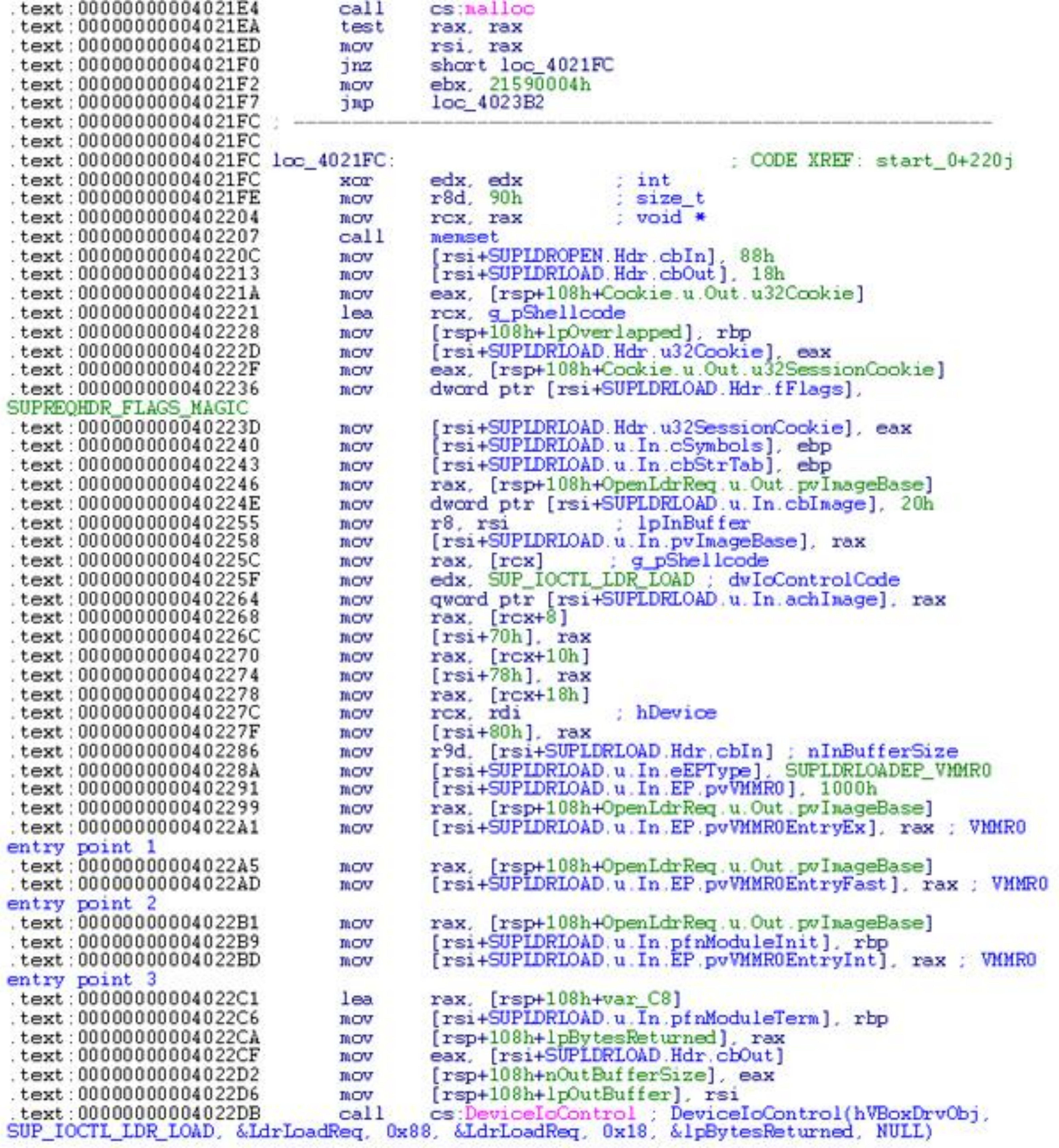
Hacking as profession

Modular, well designed software

Strong knowledge of OS internals

Hidden deep in kernel, no traces

DRM protected



```
.text:00000000004021E4        call    cs:malloc
.text:00000000004021EA        test    rax, rax
.text:00000000004021ED        mov     rsi, rax
.text:00000000004021F0        jnz     short loc_4021FC
.text:00000000004021F2        mov     ebx, 21590004h
.text:00000000004021F7        jmp     loc_4023B2
.text:00000000004021FC ; ---------------------------------------------------------------------------
.text:00000000004021FC
.text:00000000004021FC loc_4021FC:                                   ; CODE XREF: start_0+220j
.text:00000000004021FC        xor     edx, edx        ; int
.text:00000000004021FE        mov     r8d, 90h        ; size_t
.text:0000000000402204        mov     rcx, rax        ; void *
.text:0000000000402207        call    memset
.text:000000000040220C        mov     [rsi+SUPLDROPEN.Hdr.cbIn], 88h
.text:0000000000402213        mov     [rsi+SUPLDRLOAD.Hdr.cbOut], 18h
.text:000000000040221A        mov     eax, [rsp+108h+Cookie.u.Out.u32Cookie]
.text:0000000000402221        lea     rcx, g_pShellcode
.text:0000000000402228        mov     [rsp+108h+lpOverlapped], rbp
.text:000000000040222D        mov     [rsi+SUPLDRLOAD.Hdr.u32Cookie], eax
.text:000000000040222F        mov     eax, [rsp+108h+Cookie.u.Out.u32SessionCookie]
.text:0000000000402236        mov     dword ptr [rsi+SUPLDRLOAD.Hdr.fFlags],
SUPREQHDR_FLAGS_MAGIC
.text:000000000040223D        mov     [rsi+SUPLDRLOAD.Hdr.u32SessionCookie], eax
.text:0000000000402240        mov     [rsi+SUPLDRLOAD.u.In.cSymbols], ebp
.text:0000000000402243        mov     [rsi+SUPLDRLOAD.u.In.cbStrTab], ebp
.text:0000000000402246        mov     rax, [rsp+108h+OpenLdrReq.u.Out.pvImageBase]
.text:000000000040224E        mov     dword ptr [rsi+SUPLDRLOAD.u.In.cbImage], 20h
.text:0000000000402255        mov     r8, rsi         ; lpInBuffer
.text:0000000000402258        mov     [rsi+SUPLDRLOAD.u.In.pvImageBase], rax
.text:000000000040225C        mov     rax, [rcx]      ; g_pShellcode
.text:000000000040225F        mov     edx, SUP_IOCTL_LDR_LOAD ; dwIoControlCode
.text:0000000000402264        mov     qword ptr [rsi+SUPLDRLOAD.u.In.achImage], rax
.text:0000000000402268        mov     rax, [rcx+8]
.text:000000000040226C        mov     [rsi+70h], rax
.text:0000000000402270        mov     rax, [rcx+10h]
.text:0000000000402274        mov     [rsi+78h], rax
.text:0000000000402278        mov     rax, [rcx+18h]
.text:000000000040227C        mov     rcx, rdi        ; hDevice
.text:000000000040227F        mov     [rsi+80h], rax
.text:0000000000402286        mov     r9d, [rsi+SUPLDRLOAD.Hdr.cbIn] ; nInBufferSize
.text:000000000040228A        mov     [rsi+SUPLDRLOAD.u.In.eEPType], SUPLDRLOADEP_VMMR0
.text:0000000000402291        mov     [rsi+SUPLDRLOAD.u.In.EP.pvVMMR0], 1000h
.text:0000000000402299        mov     rax, [rsp+108h+OpenLdrReq.u.Out.pvImageBase]
.text:00000000004022A1        mov     [rsi+SUPLDRLOAD.u.In.EP.pvVMMR0EntryEx], rax ; VMMR0
entry point 1
.text:00000000004022A5        mov     rax, [rsp+108h+OpenLdrReq.u.Out.pvImageBase]
.text:00000000004022AD        mov     [rsi+SUPLDRLOAD.u.In.EP.pvVMMR0EntryFast], rax ; VMMR0
entry point 2
.text:00000000004022B1        mov     rax, [rsp+108h+OpenLdrReq.u.Out.pvImageBase]
.text:00000000004022B9        mov     [rsi+SUPLDRLOAD.u.In.pfnModuleInit], rbp
.text:00000000004022BD        mov     [rsi+SUPLDRLOAD.u.In.EP.pvVMMR0EntryInt], rax ; VMMR0
entry point 3
.text:00000000004022C1        lea     rax, [rsp+108h+var_C8]
.text:00000000004022C6        mov     [rsi+SUPLDRLOAD.u.In.pfnModuleTerm], rbp
.text:00000000004022CA        mov     [rsp+108h+lpBytesReturned], rax
.text:00000000004022CF        mov     eax, [rsi+SUPLDRLOAD.Hdr.cbOut]
.text:00000000004022D2        mov     [rsp+108h+nOutBufferSize], eax
.text:00000000004022D6        mov     [rsp+108h+lpOutBuffer], rsi
.text:00000000004022DB        call    cs:DeviceIoControl ; DeviceIoControl(hVBoxDrvObj,
SUP_IOCTL_LDR_LOAD, &LdrLoadReq, 0x88, &LdrLoadReq, 0x18, &lpBytesReturned, NULL)
```

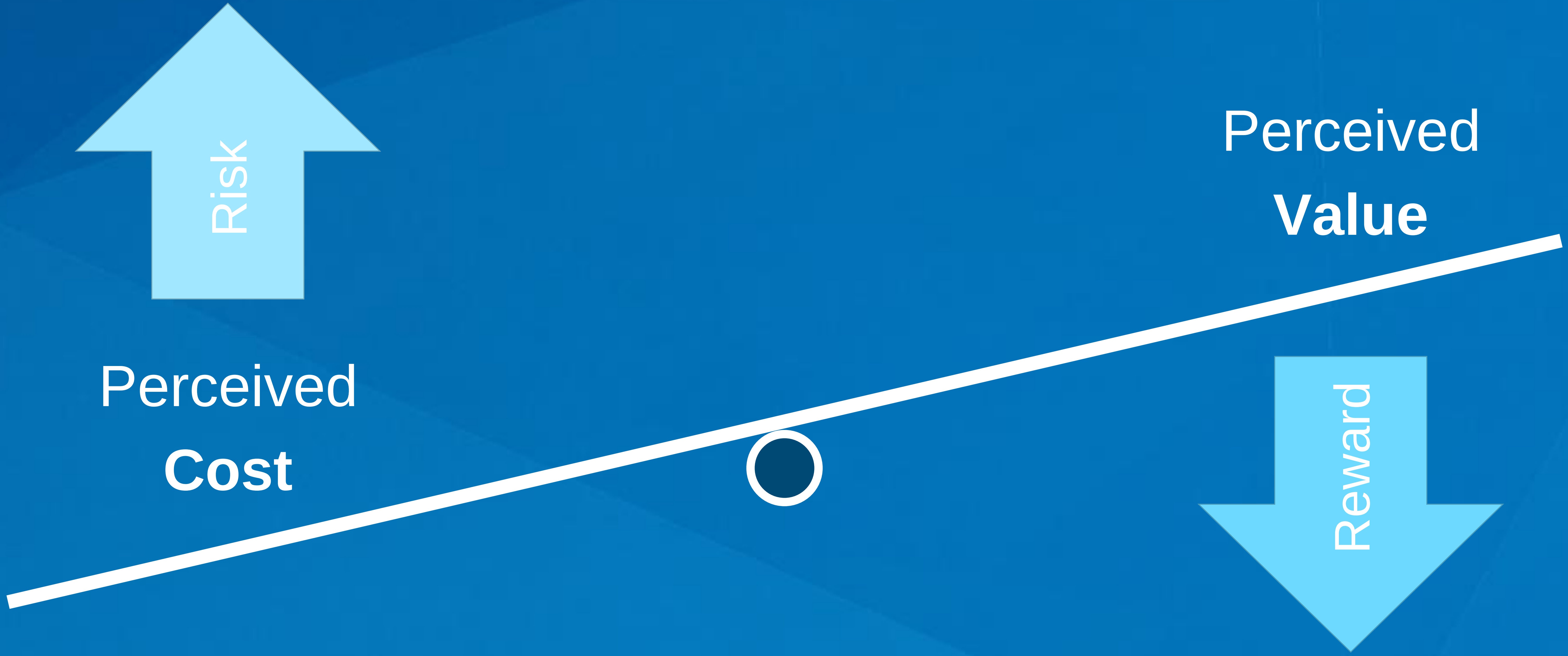
ANTI-CHEATING

┬──┬ ノ(゜-゜ノ)

[Turret Activated]

Why not cheat?

Anti-cheat Strategies

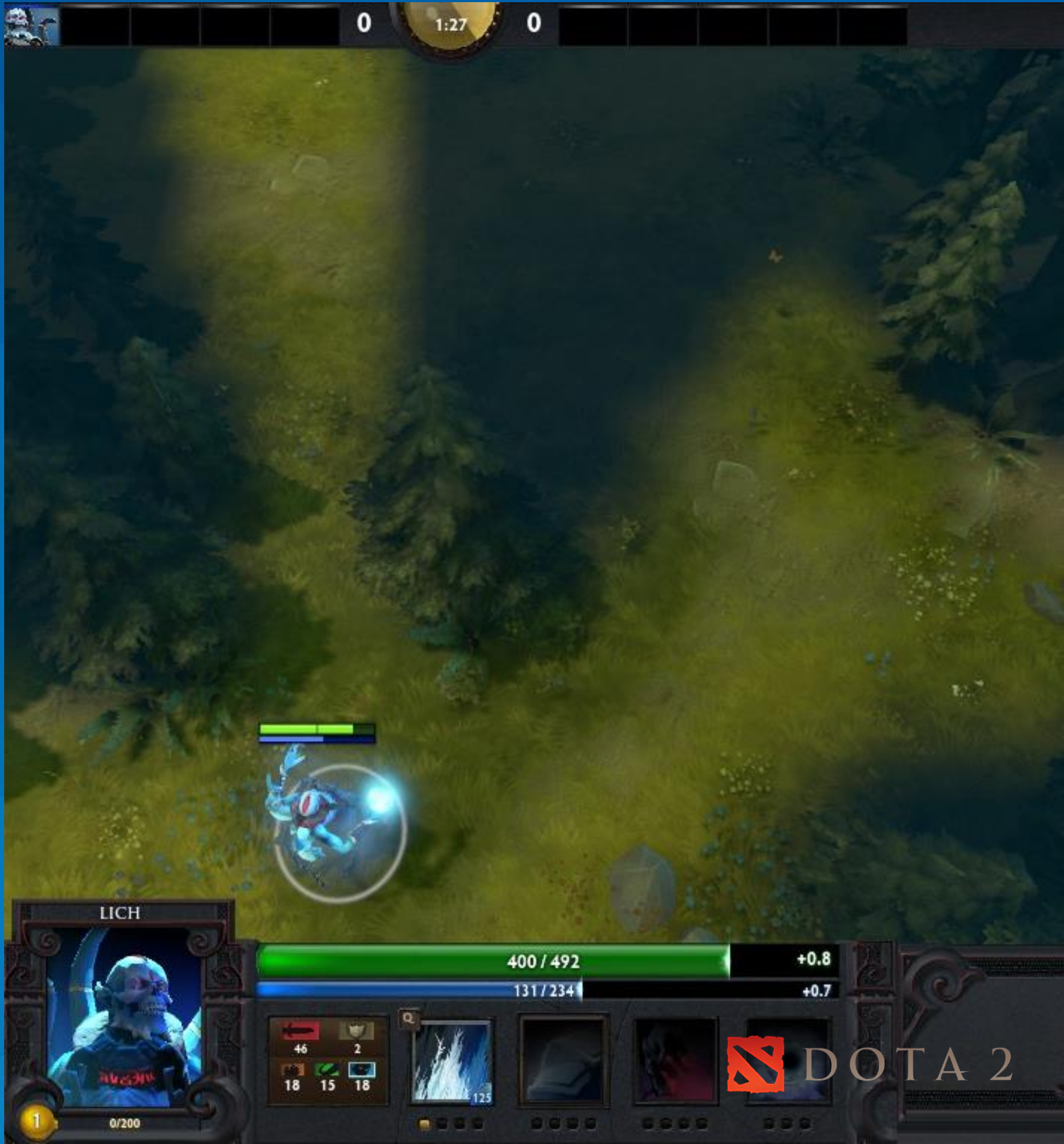


Reduced Reward

Decrease value of cheating

→ Anti-cheat by design

Authoritative game server



Reduced Reward

Decrease value of cheating

→ Anti-cheat by design

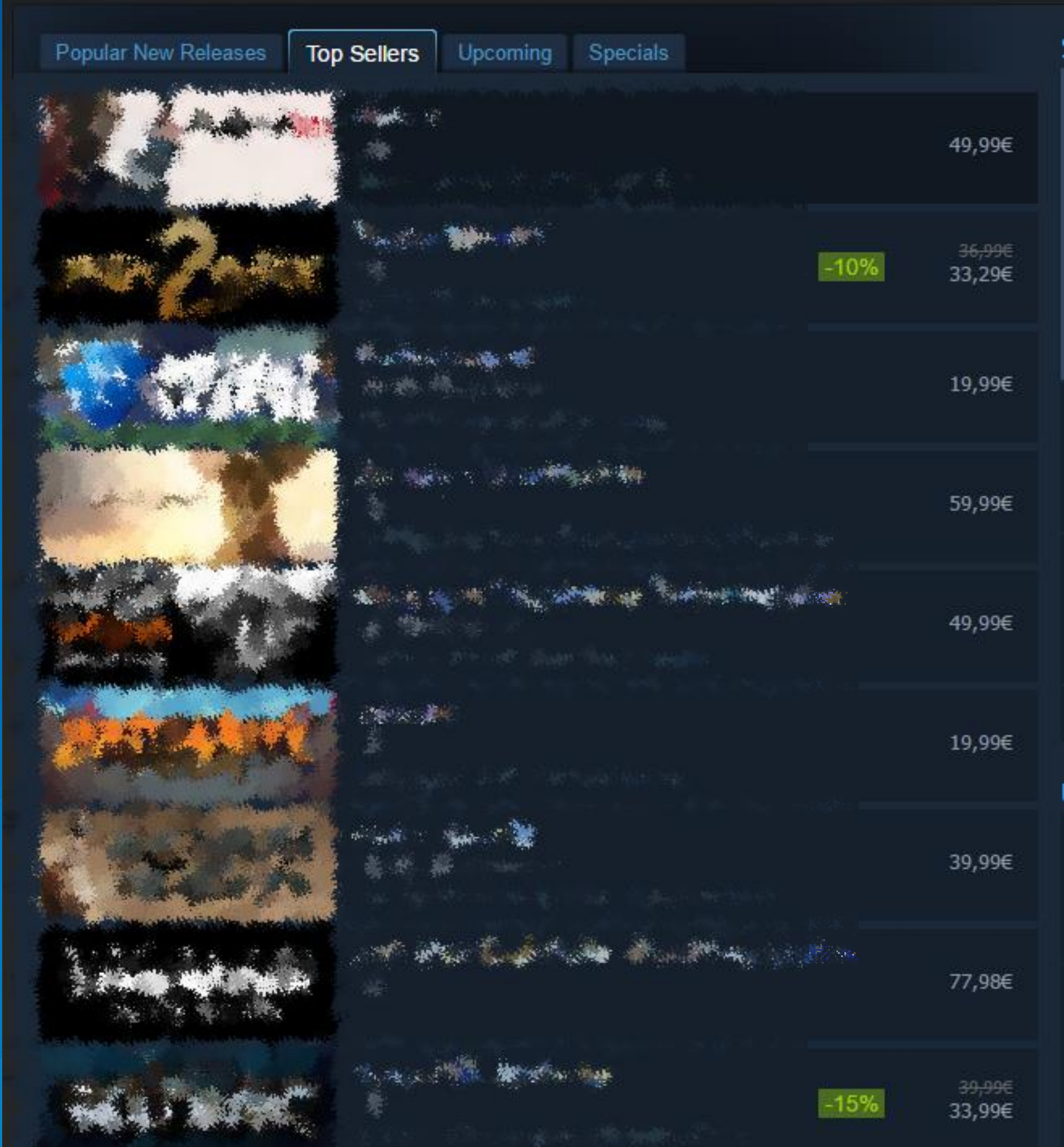
Authoritative game server

Game Mechanics

Increased Risk

Grow cost incurred from cheating

Game price



49,99€

-10% ~~36,99€~~ 33,29€

19,99€

59,99€

49,99€

19,99€

39,99€

77,98€

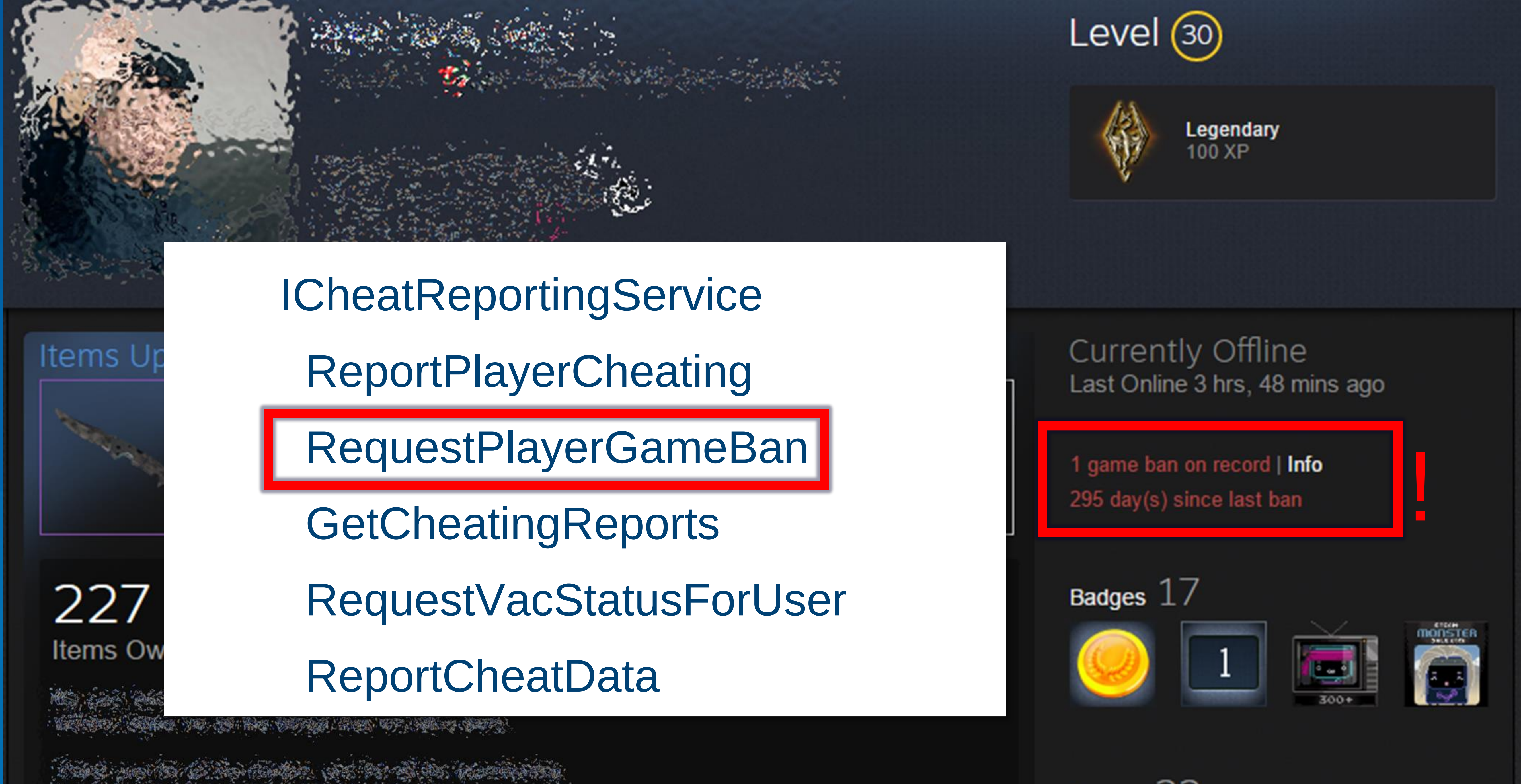
-15% ~~39,99€~~ 33,99€

Increased Risk

Grow cost incurred from cheating

Game price

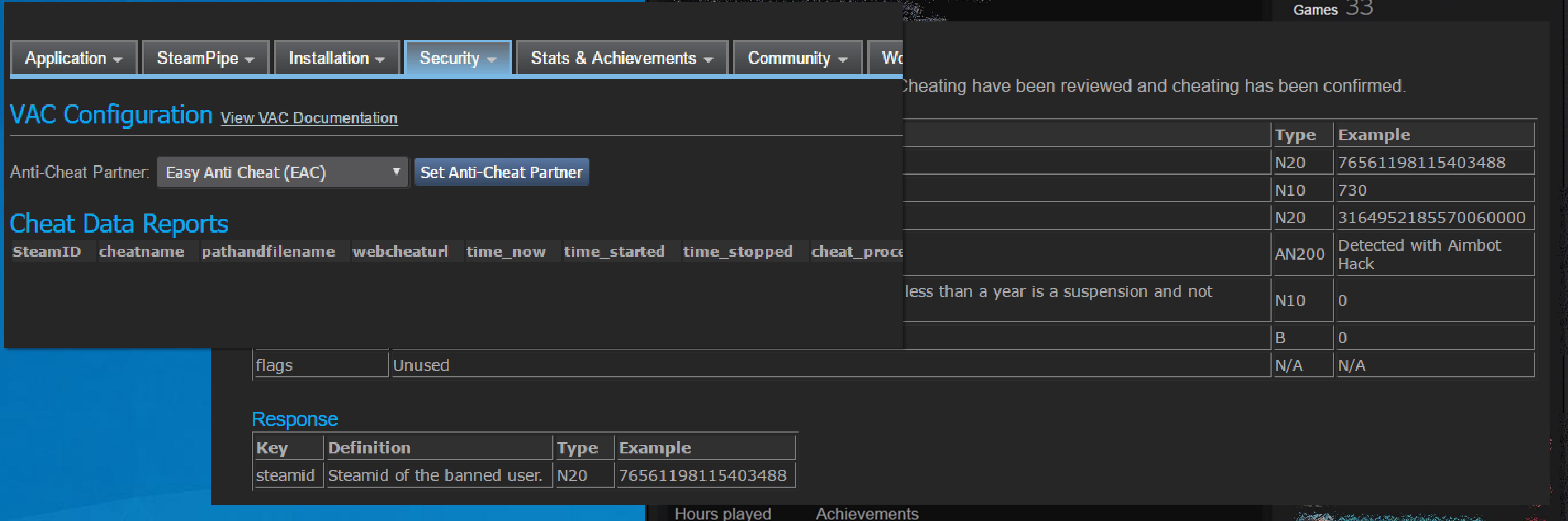
Account value



Level 30
Legendary
100 XP
Items Up
227
Items Ow
Currently Offline
Last Online 3 hrs, 48 mins ago
1 game ban on record | Info
295 day(s) since last ban
!
Badges 17
1

ICheatReportingService

- ReportPlayerCheating
- RequestPlayerGameBan
- GetCheatingReports
- RequestVacStatusForUser
- ReportCheatData



VAC Configuration View VAC Documentation

Anti-Cheat Partner: Easy Anti Cheat (EAC)

Cheat Data Reports

SteamID	cheatname	pathandfilename	webcheaturl	time_now	time_started	time_stopped	cheat_proce

…heating have been reviewed and cheating has been confirmed.

		Type	Example
		N20	76561198115403488
		N10	730
		N20	3164952185570060000
		AN200	Detected with Aimbot Hack
	less than a year is a suspension and not	N10	0
		B	0
flags	Unused	N/A	N/A

Response

Key	Definition	Type	Example
steamid	Steamid of the banned user.	N20	76561198115403488

Increased Risk

Grow cost incurred from cheating

Game price

Account value

Ranked matchmaking
and tiered gameplay

Increased Risk

Grow cost incurred from cheating

Game price

Account value

Ranked matchmaking
and tiered gameplay

Reduced supply inflates cheat price

ANTI-CHEAT AS A SERVICE

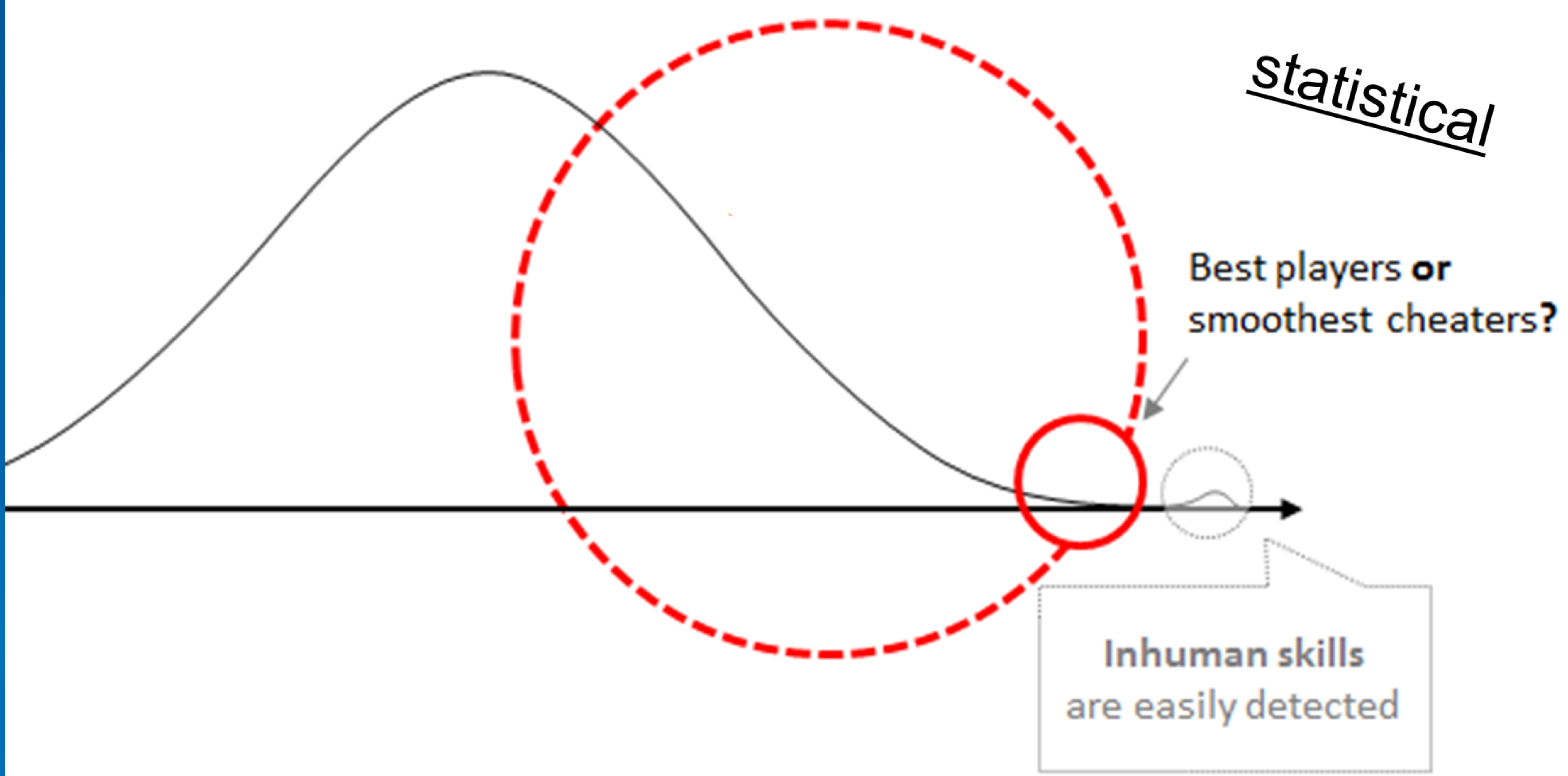
┬──┬ ノ(゜-゜ノ)

Anti-Cheat Services

Raising the bar for cheating

Detect cheats

statistics vs signature vs heuristic



Anti-Cheat Services

Raising the bar for cheating

Detect cheats

statistics vs signature vs heuristic

Discover cheats

reporting vs manual vs automated

Anti-Cheat Services

Raising the bar for cheating

Detect cheats

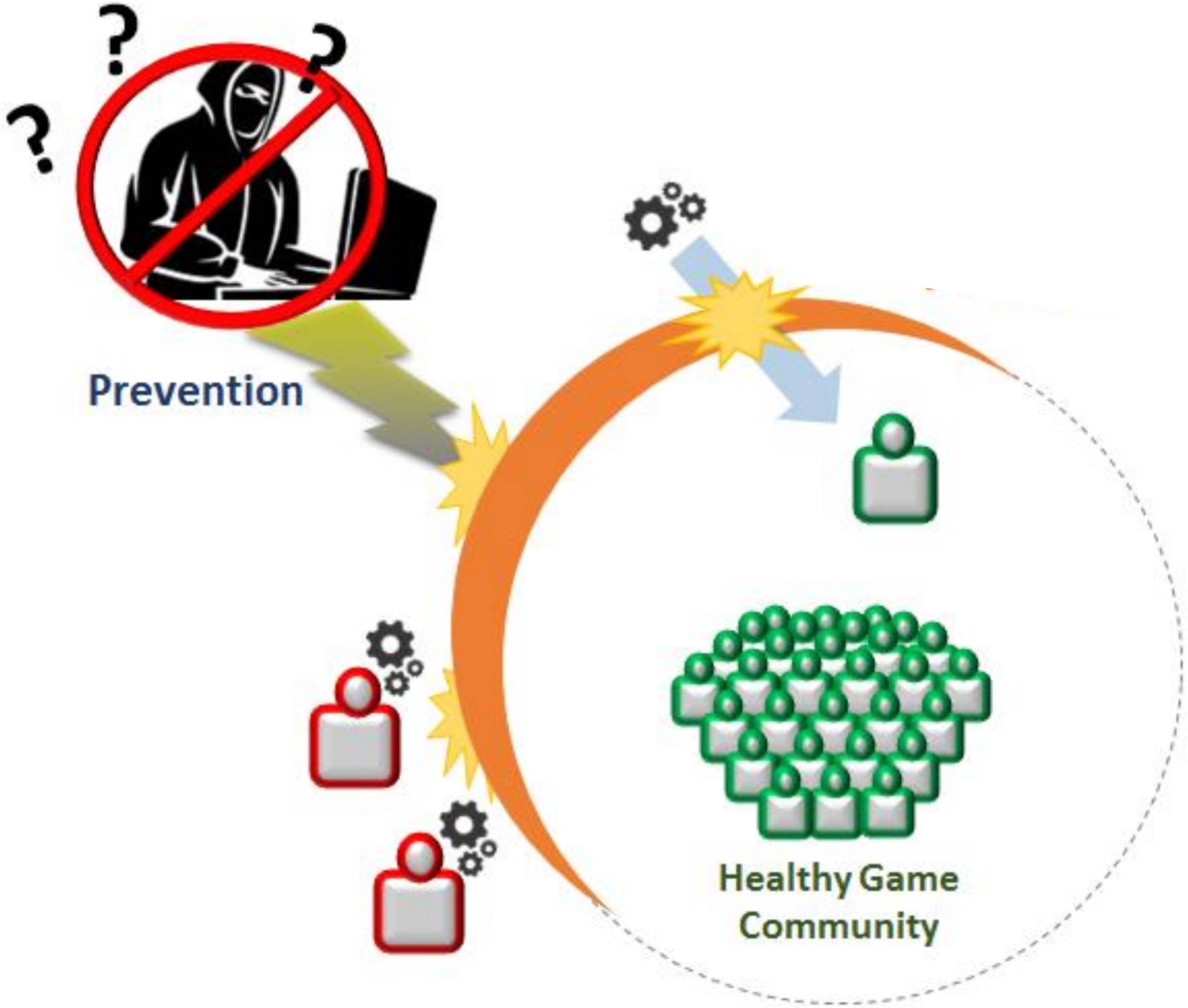
statistics vs signature vs heuristic

Discover cheats

reporting vs manual vs automated

Prevent cheats

code obfuscation vs sandbox



Anti-Cheat Services

Raising the bar for cheating

Detect cheats

statistics vs signature vs heuristic

Discover cheats

reporting vs manual vs automated

Prevent cheats

code obfuscation vs sandbox

Ship updates

game updates vs independent

Doing it yourself?

Some quick advice

Protect company assets

- Machine isolation
- Network isolation
- VPN

Protect sensitive information

- Gmail, Skype, Outlook
- Payment data
- Source code

Scope, allocate

- It never ends

STAYING IN CONTROL

(づ｡◕‿‿◕｡)づ

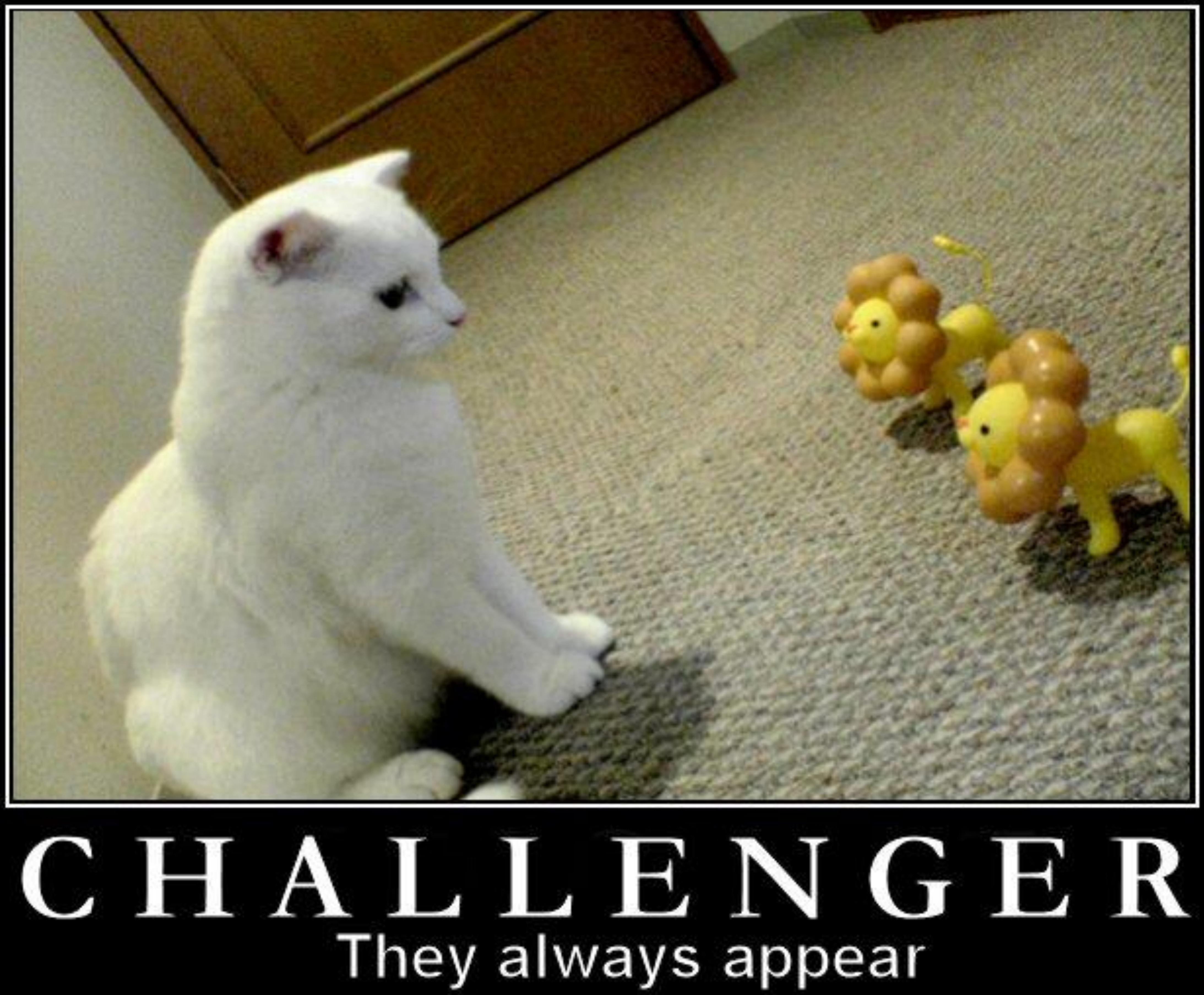
What to do?

Staying in control

Community management

Plan ahead

Disconnect



What to do?

Community management

Community management

Plan ahead

Disconnect

Acknowledge and show commitment

Avoid added publicity for cheating

No promises or claims

Keep the focus on game content

What to do?

Plan ahead

Community management

Plan ahead

Disconnect

During early design phases

Trust client as little as possible

React quick to exploits

What to do?

Disconnect

Community management

Plan ahead

Disconnect

- Don’t engage in warfare
- Separate the people from the problem
- Isolated task force team
- Don’t underestimate
- Cheating is not solved overnight

Always behave like a duck. Keep calm and unruffled on the surface, but paddle like hell underwater.