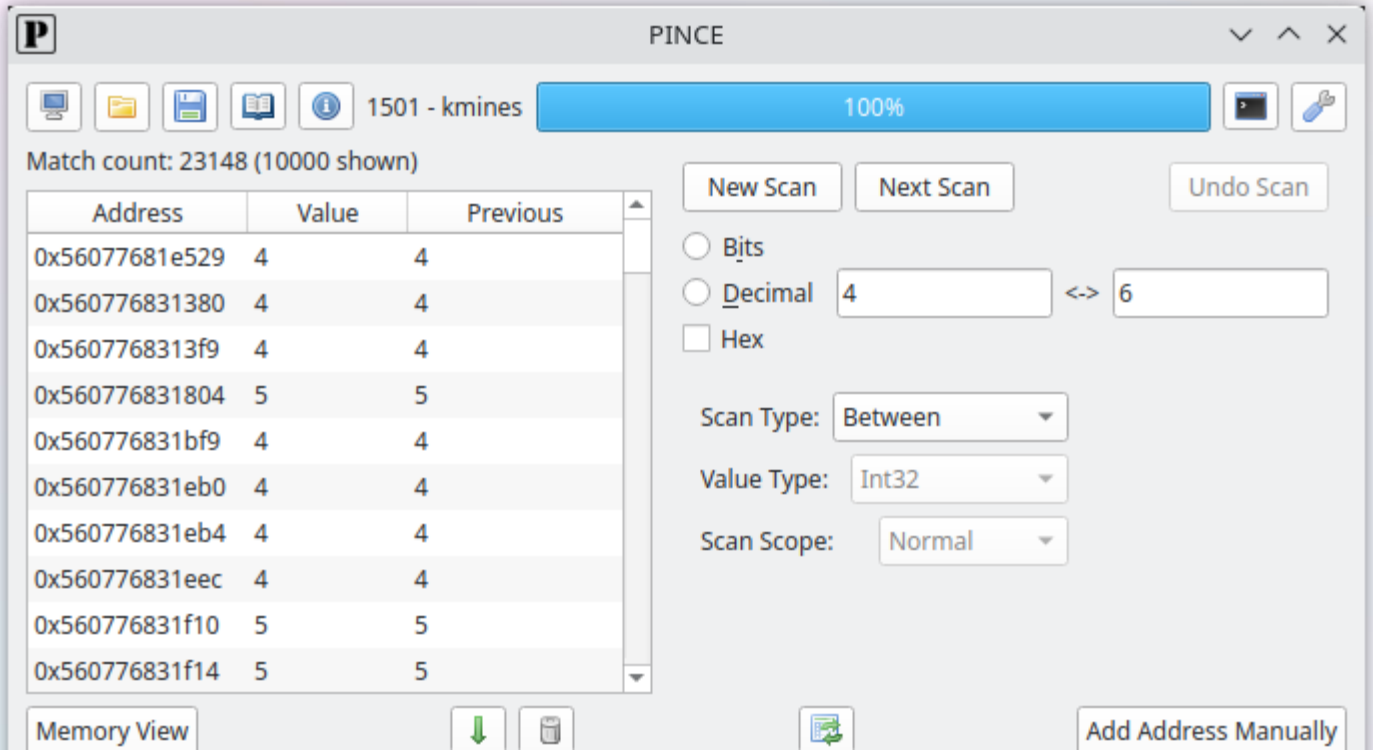
Protecting Godot Games from hackers

26/02/2024

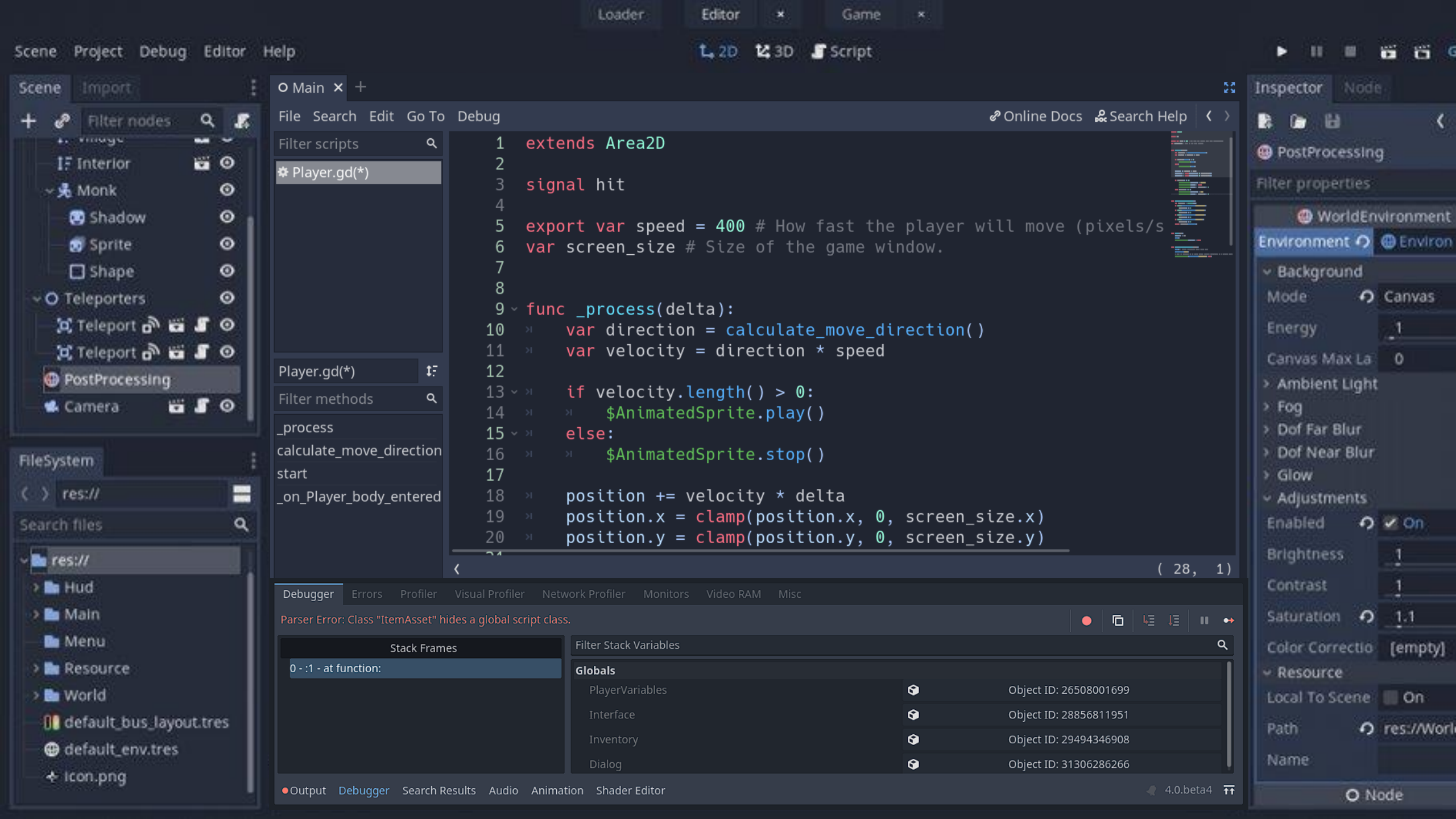
My game for a CtF challenge: Flag Quest

- My game for a CtF challenge: Flag Quest
- **Goal is to do memory analysis/modification with CheatEngine/Pince**



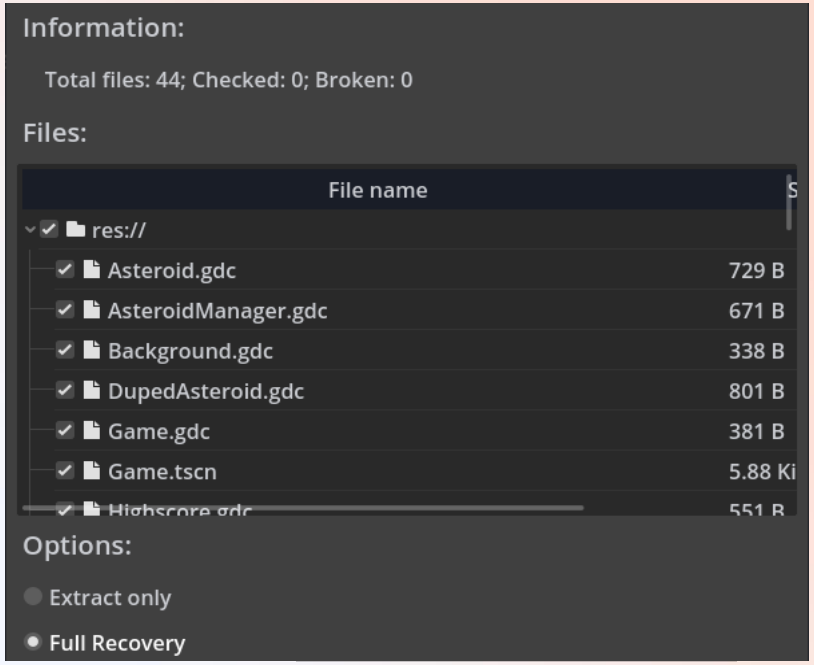
- My game for a CtF challenge
- Goal is to do memory analysis/modification
- **Made with Godot Engine:**
  lightweight, simple to use, Open-source.


Loader
Editor
Game
Scene Project Debug Editor Help
2D 3D Script
Scene Import
Filter nodes
Interior
Monk
Shadow
Sprite
Shape
Teleporters
Teleport
Teleport
PostProcessing
Camera
Main
World
View
149.8 %
GODOT
DOJO
FileSystem
res://
Search files
res://
Hud
Main
Menu
Resource
World
default_bus_layout.tres
default_env.tres
icon.png
Debugger Errors Profiler Visual Profiler Network Profiler Monitors Video RAM Misc
Parser Error: Class "ItemAsset" hides a global script class.
Stack Frames
0 - :1 - at function:
Filter Stack Variables
Globals
PlayerVariables Object ID: 26508001699
Interface Object ID: 28856811951
Inventory Object ID: 29494346908
Dialog Object ID: 31306286266
Output Debugger Search Results Audio Animation Shader Editor
4.0.beta4
Inspector Node
PostProcessing
Filter properties
WorldEnvironment
Environment Environ
Background
Mode Canvas
Energy 1
Canvas Max La 0
Ambient Light
Fog
Dof Far Blur
Dof Near Blur
Glow
Adjustments
Enabled On
Brightness 1
Contrast 1
Saturation 1.1
Color Correctio [empty]
Resource
Local To Scene On
Path res://Worl
Name
Node


Loader
Editor
Game
Scene Project Debug Editor Help
2D 3D Script
Scene Import
Filter nodes
Interior
Monk
Shadow
Sprite
Shape
Teleporters
Teleport
Teleport
PostProcessing
Camera
FileSystem
res://
Search files
res://
Hud
Main
Menu
Resource
World
default_bus_layout.tres
default_env.tres
icon.png
Main
File Search Edit Go To Debug
Online Docs Search Help
Filter scripts
Player.gd(*)
Player.gd(*)
Filter methods
_process
calculate_move_direction
start
_on_Player_body_entered
1 extends Area2D
2
3 signal hit
4
5 export var speed = 400 # How fast the player will move (pixels/s
6 var screen_size # Size of the game window.
7
8
9 func _process(delta):
10 var direction = calculate_move_direction()
11 var velocity = direction * speed
12
13 if velocity.length() > 0:
14 $AnimatedSprite.play()
15 else:
16 $AnimatedSprite.stop()
17
18 position += velocity * delta
19 position.x = clamp(position.x, 0, screen_size.x)
20 position.y = clamp(position.y, 0, screen_size.y)
(28, 1)
Debugger Errors Profiler Visual Profiler Network Profiler Monitors Video RAM Misc
Parser Error: Class "ItemAsset" hides a global script class.
Stack Frames
0 - :1 - at function:
Filter Stack Variables
Globals
PlayerVariables Object ID: 26508001699
Interface Object ID: 28856811951
Inventory Object ID: 29494346908
Dialog Object ID: 31306286266
Output Debugger Search Results Audio Animation Shader Editor
4.0.beta4
Inspector Node
PostProcessing
Filter properties
WorldEnvironment
Environment Environ
Background
Mode Canvas
Energy 1
Canvas Max La 0
Ambient Light
Fog
Dof Far Blur
Dof Near Blur
Glow
Adjustments
Enabled On
Brightness 1
Contrast 1
Saturation 1.1
Color Correctio [empty]
Resource
Local To Scene On
Path res://Worl
Name
Node

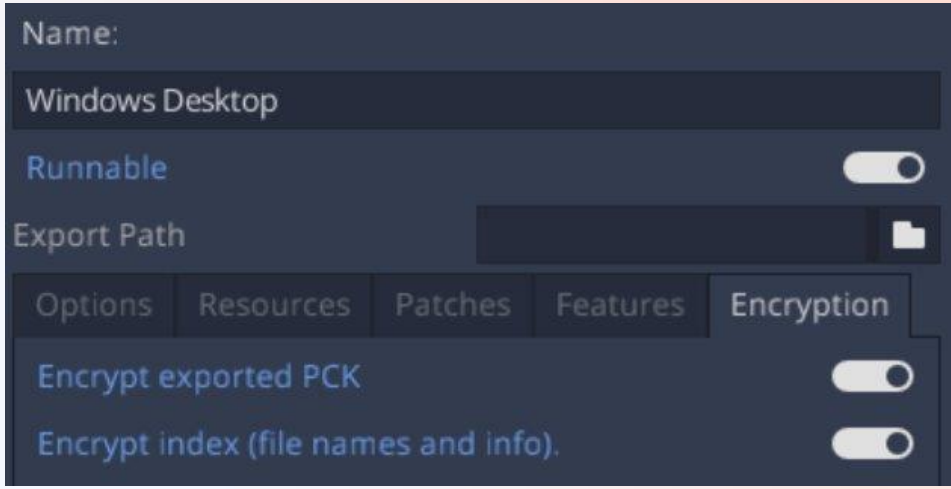
What prevents players from reversing the binary?

- **Godot games are entirely reversable with Gdsdecomp, as code is interpreted.**



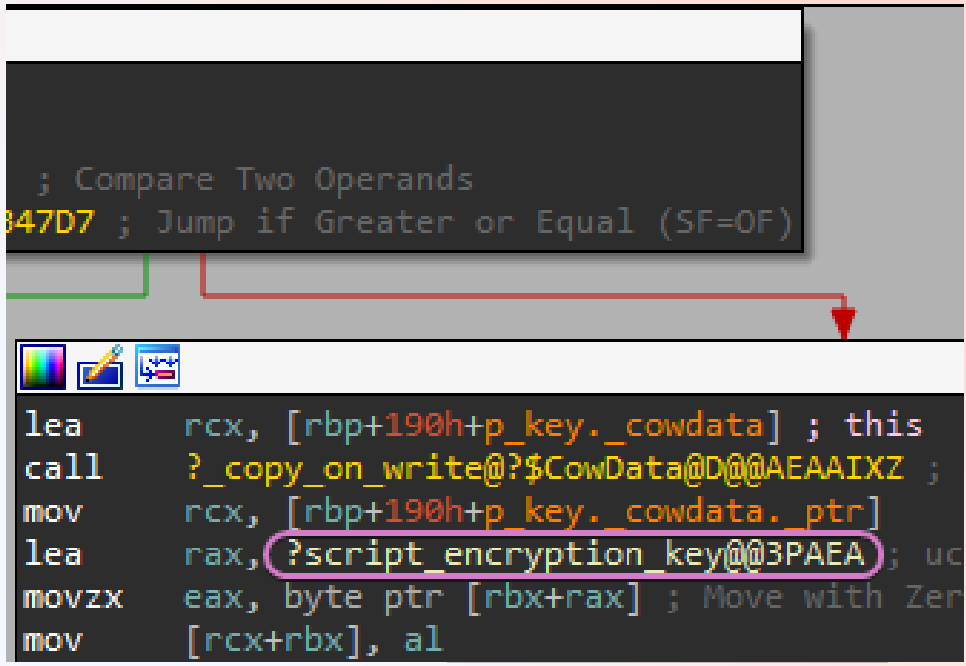
What prevents players from reversing the binary?

- Gdsdecomp reverses Godot projects
- **Binaries can be encrypted with an AES key.**
  (needs engine recompilation)



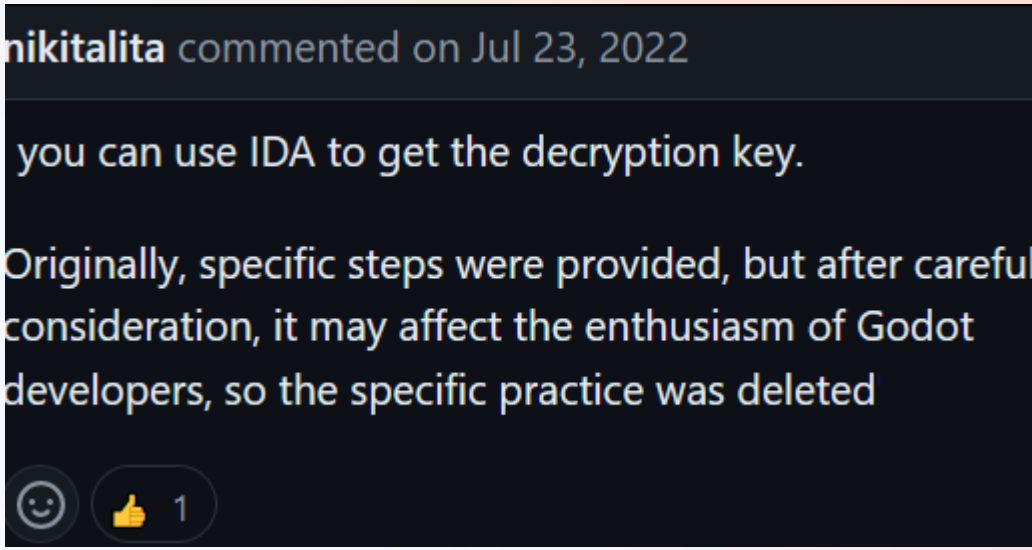
What prevents players from reversing the binary?

- Gdsdecomp reverses Godot projects
- Binaries can be encrypted
- **The key is inside the binary, and can be extracted**



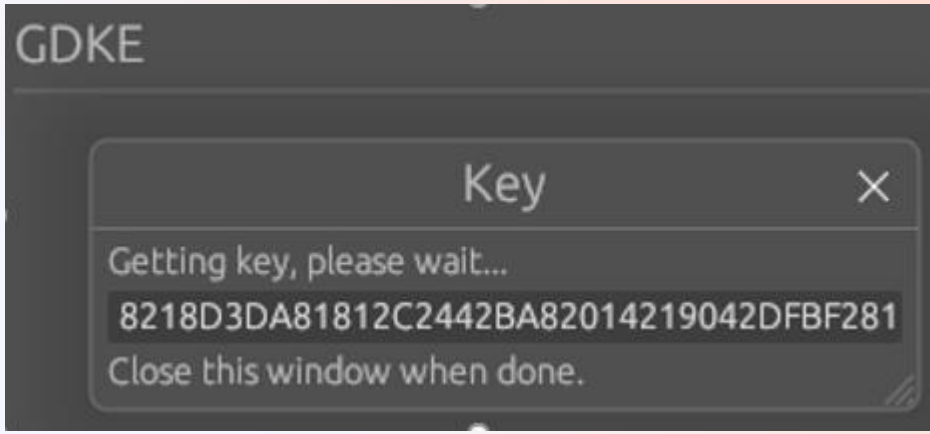
What prevents players from reversing the binary?

- Gdsdecomp reverses Godot projects
- Binaries can be encrypted
- The key is inside the binary,
- **Gdsdecomp dev won't give documentation on how to extract it.**



What prevents players from reversing the binary?

- Gdsdecomp reverses Godot projects
- Binaries can be encrypted
- The key is inside the binary,
- no documentation on how to extract it.
- **But someone else did it: gdke**



What do?

GDscript > Obfuscation

cherriesandmochi / **gdmaim**

```gdscript
extends Node

signal my_signal(param1 : int)
enum MyEnum { FIRST_KEY, SECOND_KEY = 3, THIRD_KEY, }
const MY_CONST : int = 1 #TODO ...

@export var my_export_var : int
var my_var : MyEnum = MyEnum.THIRD_KEY

# Do something
func my_func(param1 : float, param2 : bool) -> void:
	my_var += 1
	if true:
		var my_var : bool
		my_var = false

	custom_setter("my_var", MY_CONST)

	var class_inst : MyClass = MyClass.new()
	class_inst.class_member = "my_var"

	var dict : Dictionary = { "my_var": 0, }
	my_var = dict.my_var

	my_signal.emit(my_var)
```

```gdscript
extends Node
signal __YCFK(__ge1l : int)
@export var __XqYA : int
var __j21W : int = 4
func __WpQR(__fgec : float, __MOKi : bool) -> void:
	__j21W += 1
	if true:
		var __vRHj : bool
		__vRHj = false
	__BECz("__j21W", 1)
	var __N7o3 : __S7_g = __S7_g.new()
	__N7o3.__69Qh = "my_var"
	var __jidx : Dictionary = { "my_var": 0, }
	__j21W = __jidx.my_var
	__YCFK.emit(__j21W)
func __BECz(name : String, value) -> void:
	set(name, value)
class __S7_g:
	var __69Qh : String
```

What do?

GDscript > Obfuscation > Intermediate language

cherriesandmochi / **gdmaim**

In Godot 4.3 (beta)

```
1   extends Node
2
3   signal my_signal(param1 : int)
4   enum MyEnum { FIRST_KEY, SECOND_KEY = 3, THIRD_KEY, }
5   const MY_CONST : int = 1 #TODO ...
6
7   @export var my_export_var : int
8   var my_var : MyEnum = MyEnum.THIRD_KEY
9
10  # Do something
11  func my_func(param1 : float, param2 : bool) -> void:
12      my_var += 1
13      if true:
14          var my_var : bool
15          my_var = false
16
17      custom_setter("my_var", MY_CONST)
18
19      var class_inst : MyClass = MyClass.new()
20      class_inst.class_member = "my_var"
21
22      var dict : Dictionary = { "my_var": 0, }
23      my_var = dict.my_var
24
25      my_signal.emit(my_var)
```

```
mov     edx,DWORD PTR [ebp-0x1c]
mov     eax,DWORD PTR [ebp-0x30]
add     eax,edx
mov     ecx,DWORD PTR [ebp-0x1c]
mov     edx,DWORD PTR [ebp-0x30]
add     edx,ecx
movzx   edx,BYTE PTR [edx]
xor     edx,0x63
mov     BYTE PTR [eax],dl
add     DWORD PTR [ebp-0x1c],0x1
mov     eax,DWORD PTR [ebp-0x1c]
cmp     eax,0x196
jbe     0x8048a8a

mov     eax,ds:0x8049348
mov     ebx,eax
mov     eax,DWORD PTR [ebp-0x30]
call    eax

sub     esp,0x4
push    0x197
push    0x0
push    DWORD PTR [ebp-0x30]
call    0xf7f0de50
add     esp,0x10
sub     esp,0xc
push    0x0
call    0xf7e157e0 <exit>


lea     esp,[ebp-0x10]
pop     ecx
```

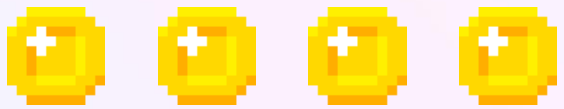
What do?

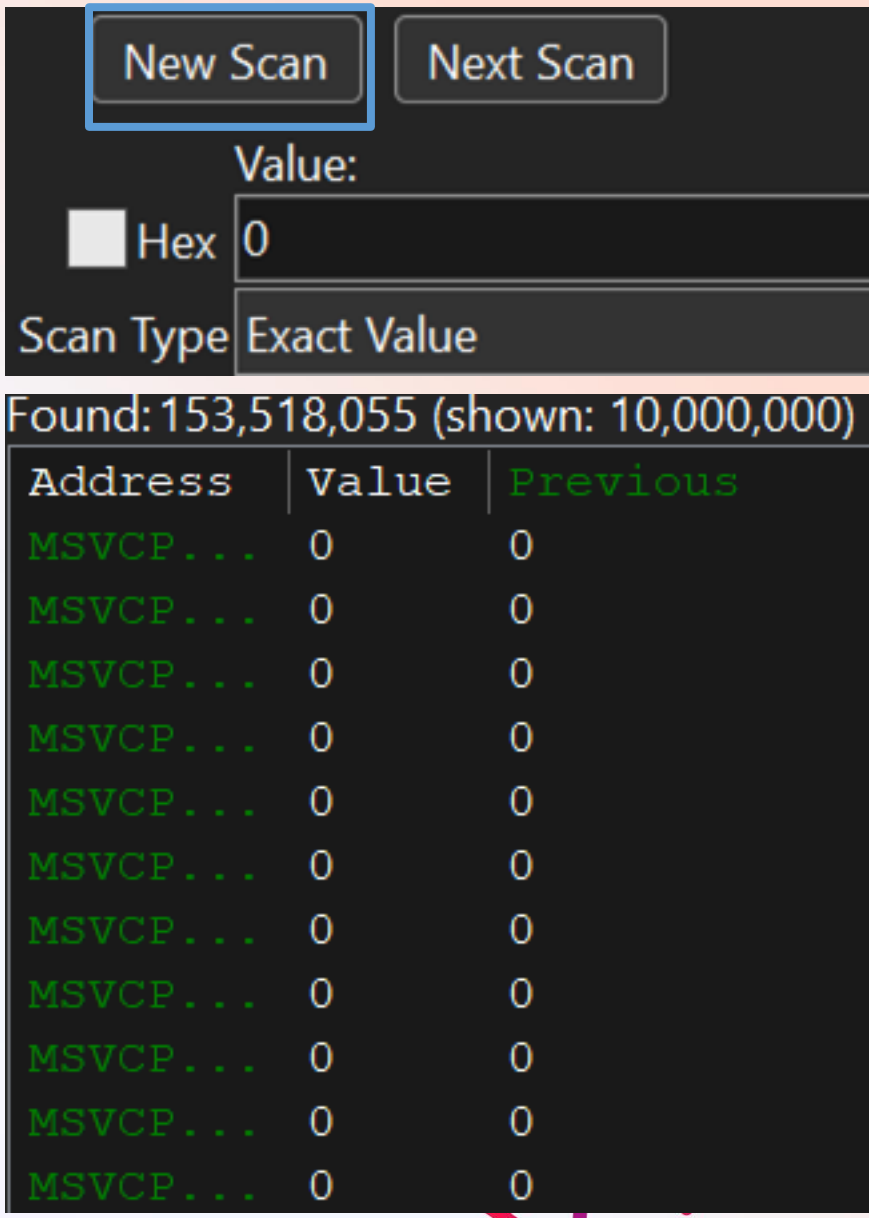
Rewrite in Rust (with GD extensions)

```rust
#[method]
fn _ready(&mut self, #[base] owner: &Area2D) {
    let viewport = owner.get_viewport_rect();
    self.screen_size = viewport.size;
    owner.hide();
}

#[method]
fn _process(&mut self, #[base] owner: &Area2D, delta: f32) {
    let animated_sprite = unsafe {
        owner
            .get_node_as::<AnimatedSprite>("animated_sprite")
            .unwrap()
    };

    let input = Input::godot_singleton();
    let mut velocity = Vector2::new(0.0, 0.0);
```

Finding values in memory

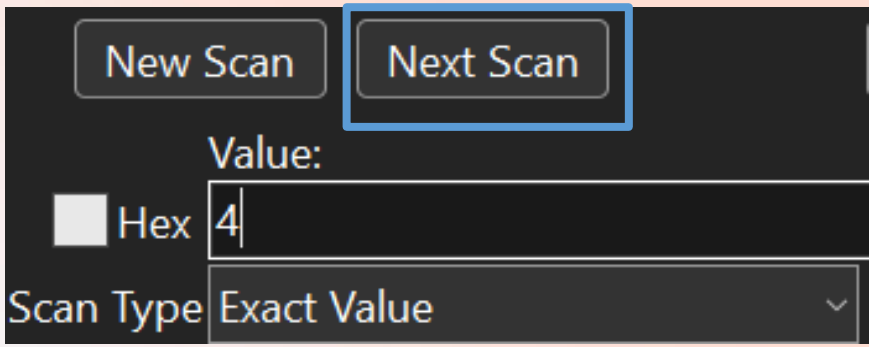
0 Coins :





Finding values in memory

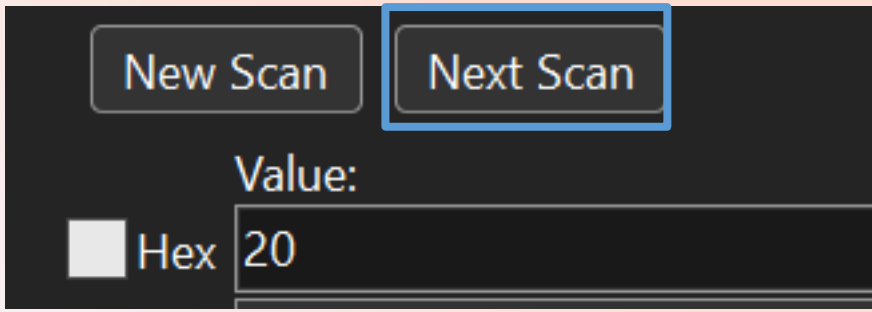
4 Coins :



Found:113

Address	Value	Previous
1318B...	0	4
1318B...	0	4
13193...	4	4
13193...	4	4
13193...	4	4
13193...	4	4
13193...	4	4
15C0A...	4	4

Finding values in memory



Found:4

Address	Value	Previous
15C0D...	20	20
15C0D...	20	20
15C0D...	20	20
15C0E...	20	20

20 Coins :

Finding values in memory

4000 Coins :

Activ	Description	Address	Type	Value
	coins	00000000		
	coins	15C0DD85978	4 Bytes	20
	coins	15C0DD859AC	4 Bytes	20
	coins	15C0EC83FD8	4 Bytes	20
	coins	15C0DD859C8	4 Bytes	20

Change Value

what value to change this to?

4000

OK

Protecting your values in memory

- Apply random operations to value
- Create canary values
- On multiplayer games:
  Never trust the client.

```
class AnticheatInt:
    var falseValue: int
    var hiddenValue: int
    var r : int
    var value: get = getter, set = setter

    func _init() -> void:
        r = RandomNumberGenerator.new().randi();

    func setter(newValue: int):
        falseValue = newValue
        hiddenValue = (newValue * 3) - r;

    func getter() -> int:
        var trueValue = ( hiddenValue + r ) / 3;
        assert(trueValue == falseValue, "ERROR: Dirty cheater");
        return trueValue;
```

Anti-Cheat Toolkit 2023

📌 Common features

Protects variables in memory.
Protects and extends Player Prefs and binary files.
Generates build code signature for tampering checks.
Detects non Play Store installations on Android.
Detects speedhacks.
Detects time cheating.
Detects 3 common wallhack types.
Detects foreign managed assemblies.
Has Obscured Prefs / Player Prefs editor.

📌 Obscured Types ▶ tutorial

Keeps your sensitive variables away from **all** memory scanners

Only 😢,
for now...

Thank you