

12 Days of Ghidra

Nathan R

[Twitter](#) | [Mastodon](#)

Day 6 – Reversing C++ Objects

Intro to C++

Object-Oriented version of C

- C is a subset of C++

Introduces:

- Classes
 - Similar in principle to C structs
 - Difference is encapsulation - public, private, and protected keywords
- Methods
 - Functions that are bound to a class/object
 - I.e. the first parameter will always be 'this'

Constructors

Called when you create a new C++ object

- `Object obj = Object();`

Defines how you create a new object of that class type

- Typically, you will see some resource initialization

new vs malloc()

In previous binaries you may have noticed calls to **malloc()**

- malloc() allocates some memory and returns a pointer to this

new serves a similar purpose to malloc()

- In addition it also calls the class constructor

```
Object* obj = new obj();
```

```
obj->method();
```

Day 6 Binary

This is a more complicated binary than before

- Requires you to understand more about the program flow than before

There is no text prompts when you run the bin

- You need to RE what information to pass to main

Suggestions:

- Pay special attention to what happens inside of constructors