```
tags: [ida, re, std_type_info_name]
game: New World
engine: Amazon Lumberyard
```

Заметки

`__std_type_info_name` тот же `typeid(*classAddress).name`, это весьма подозрительный метод из-за того, что редко встречается необходимость получать имя класса игре.

Рассмотрим использования этого метода на примере New World которая использует Lumberyard engine[1]

В этой игре название классов хранятся в массиве, который используется `__std_type_info_name`, чтобы после передать название класса в метод для генерации хеша по имени класса для дальнейшего сопоставления, и если хеш совпадает метод возвращает адрес структуры.

Пример

В коде это выглядит так:

```
array = qword_14638EF90;
classNameHash = 0xCBF29CE484222325ui64; // default
classNameLenght = -1i64;
do
  ++classNameLenght;
while ( className[classNameLenght] );
for ( ; classNameLenght; --classNameLenght )
{
  char = *className++;
  classNameHash = 0x100000001B3i64 * (char ^ classNameHash);
}
_classNameHash = classNameHash;
```

Перепишем на Python для повышения читабельности:

```
def generateHashByClassName(className):
        classNameLenght = len(className) - 1
        classNameHash = 0xCBF29CE484222325
        for idx in range(classNameLenght):
                classNameHash = (0x100000001B3 * (ord(className[idx]) ^
classNameHash)) & 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

        return ((pair128(classNameHash, classNameHash) * 0xDE5FB9D2630458E9)
>> 64) & 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

def pair128(high, low):
         return (high << 64 | low)
```

Для примера сгенерируем хеш для [класса PlayerRegistry]:

```
hex(generateHashByClassName("PlayerRegistry"))
>>> 0x668f0ec14ac79076fc6d4f6cf58bf59c
```

Если углубляться в код, то игра вычисляет адрес дальше по коду таким образом:

```
def getIndexByHash(a1):
  return (__PAIR128__(a1, a1) * 0xDE5FB9D2630458E9ui64) >> 64
...
v6 = (array->qword60[0x10 * (getIndexByHash(*p_classNameHash) & array-
>qword58)]);
```

`array->qword60` является указателем на массив адресов всех существуюущих классов. А `array->qword58` ограничителем индекса.

Результат

- Подобное использование `type_info_name` в основном используется для генерации хеша по имени класса для дальнейшего сопоставление из словаря и получения адреса структуры.
- `__std_type_info_name` можно найти сразу в таблице импорта.

---

1. https://github.com/aws/lumberyard↩