How do I RE object oriented code (and you should too)

Milan Bohacek

REcon 2014

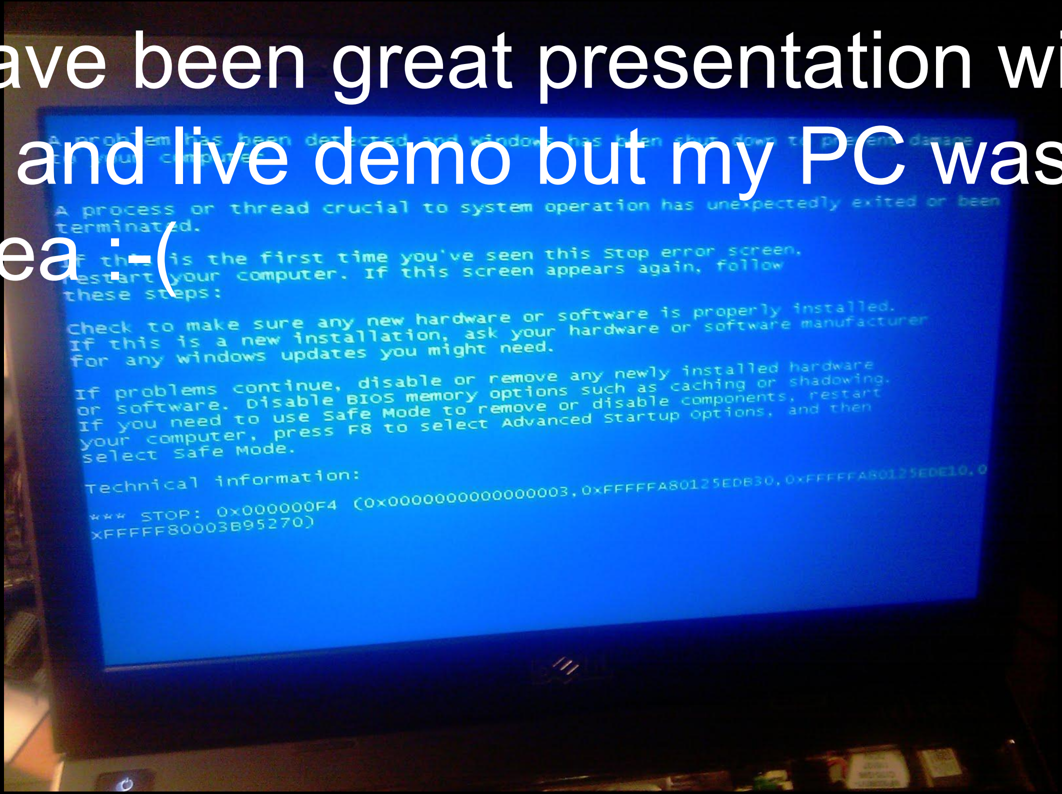
.short bio

Milan is

- PhD student at Charles University in Prague
- Part time malware analyst at avast! software
- IDA enthusiast
- without working laptop :-(

.apology

here should have been great presentation with many pictures and live demo but my PC was against that idea :-(



```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

A process or thread crucial to system operation has unexpectedly exited or been
terminated.

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup options, and then
select Safe Mode.

Technical information:

*** STOP: 0x000000F4 (0x0000000000000003,0xFFFFFA80125EDB30,0xFFFFFA80125EDE10,0
xFFFFF80003B95270)
```

.my usual line of work

1. unpack a binary
2. analyze it using Hex-Rays
3. find used cryptography
4. use algebra / common sense to check for bugs in the cryptography
5. ???
6. profit

.definition

Object-oriented programming (OOP) is a programming paradigm that represents the concept of "objects" that have data fields (attributes that describe the object) and associated procedures known as methods.

Wikipedia

.definition

Reverse engineer’s worst nightmare.

Milan

.challenge

Compile / get your favourite OO code and post a link on twitter with hashtag #reconmtl.

No malware, no obfuscation, no monkey business, < 50KB, x86 || x64 || arm.

I will try to look at it if I have time.

.basic workflow

1. open a function in hex-rays
2. identify *this* pointer
3. create a structure that reflects memory access relative to *this* pointer
4. find all functions that also have *this* as an argument
5. goto 1.
6. merge all generated structures into one

(demo)

I’m getting tired just by looking at this list.

.solution!

IDA plugins FTW!

1) IDA had “Create new struct type”
2) So I RE the way this worked and added more features
3) I ended up with a few “hacks”

.solution!

```
#if IDA_SDK_VERSION <= 610
template <typename T, int addr> class C
{
public:
	T * call;
	C():call((T*)addr){};
	T* operator()() { return call; }
};

extern C<qstring  __cdecl (tinfo_t *a2, int offset), 0x17035E90> create_field_name;
...
#endif
```

.solution

And this worked, but only for me.

(Every IDA user has private build)

Then I bugged Ilfak until he exported the functions I wanted.

.workflow with hexrays_tools

1. open a function in hex-rays
2. select *this* pointer
3. let the plugin gather all informations about an object pointed to by *this* pointer
4. ask the plugin for next function to scan
5. Once you gathered enough information let the plugin create the final object structure.

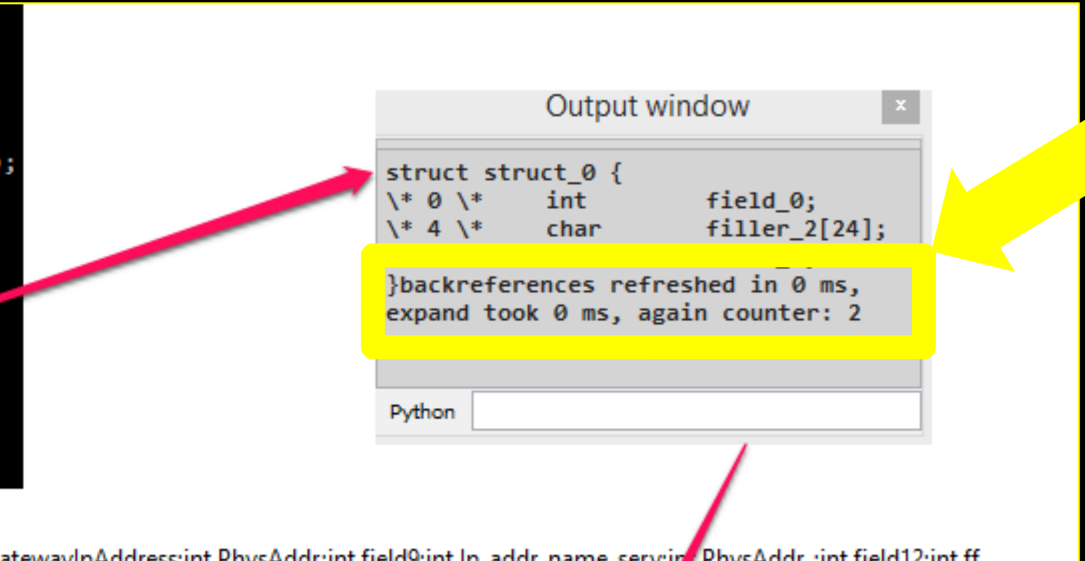
(demo)

.caveats

- simple assignments - easy to solve
- structures inside structures
- virtual tables
- negative offsets

.easter eggs

REcon 2013 HexRaysCodeXplorer
Aleksandr Matrosov & Eugene Rodionov
https://raw.githubusercontent.com/REhints/HexRaysCodeXplorer/master/img/6.png



```
struct struct_0 {
\* 0 \*     int           field_0;
\* 4 \*     char          filler_2[24];
}backreferences refreshed in 0 ms,
expand took 0 ms, again counter: 2
```

```
atewayIpAddress:int PhysAddr:int field9:int Ip_addr_name_serv:int PhysAddr_:int field12:int ff
```

HRCX screenshot contains comments generated by hexrays_tools.
Most probable cause is the presence of hexrays_tools.plw in their ida\plugins directory.

.QA

questions anyone?

.end

Thank you for your attention!

Thanks

Igor for providing me with his laptop.
Arnaud for promptly fixing bugs I find.
Ilfak for being awesome.

.contacts

milan.bohacek+re2014@gmail.com