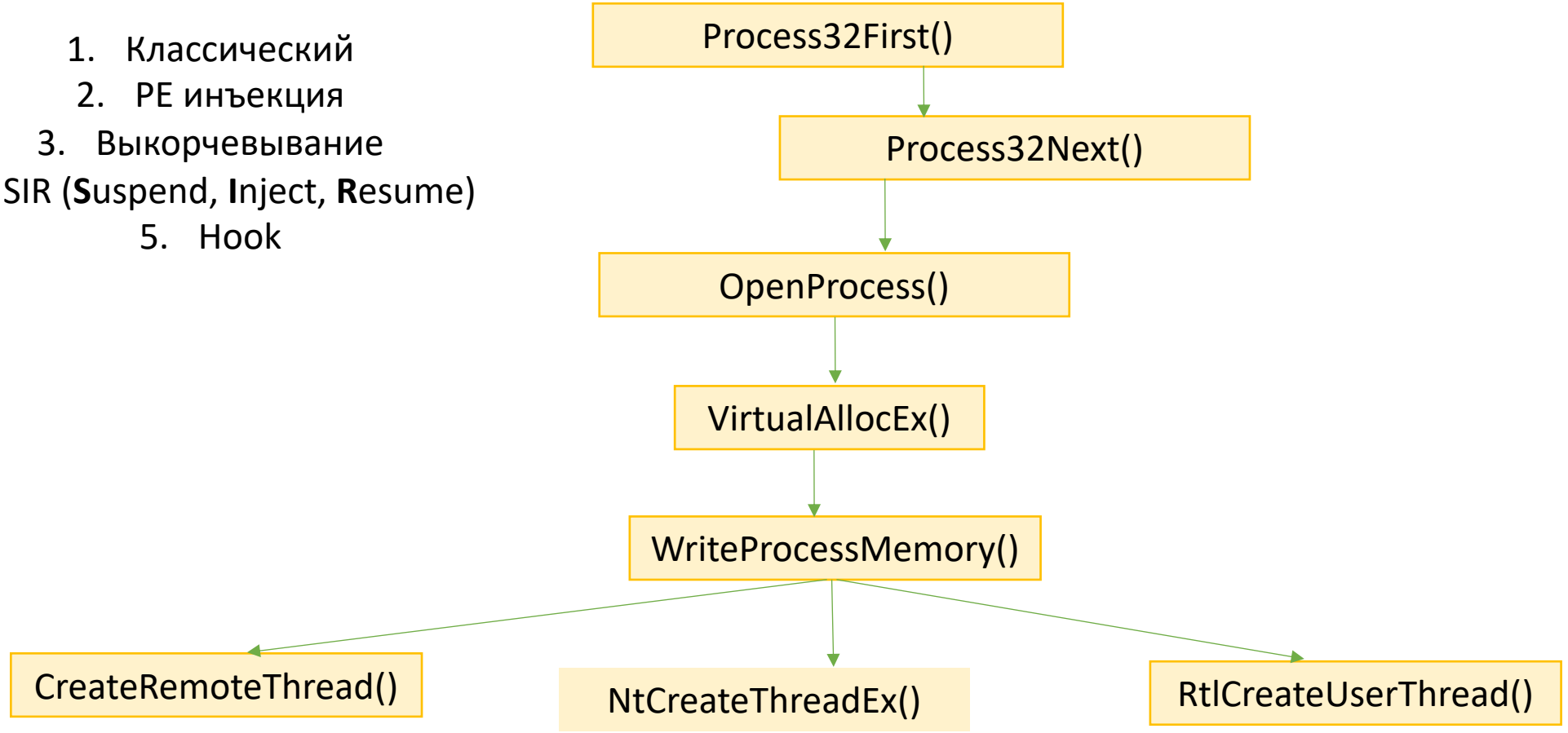
Способы внедрения в процесс

Часть 2

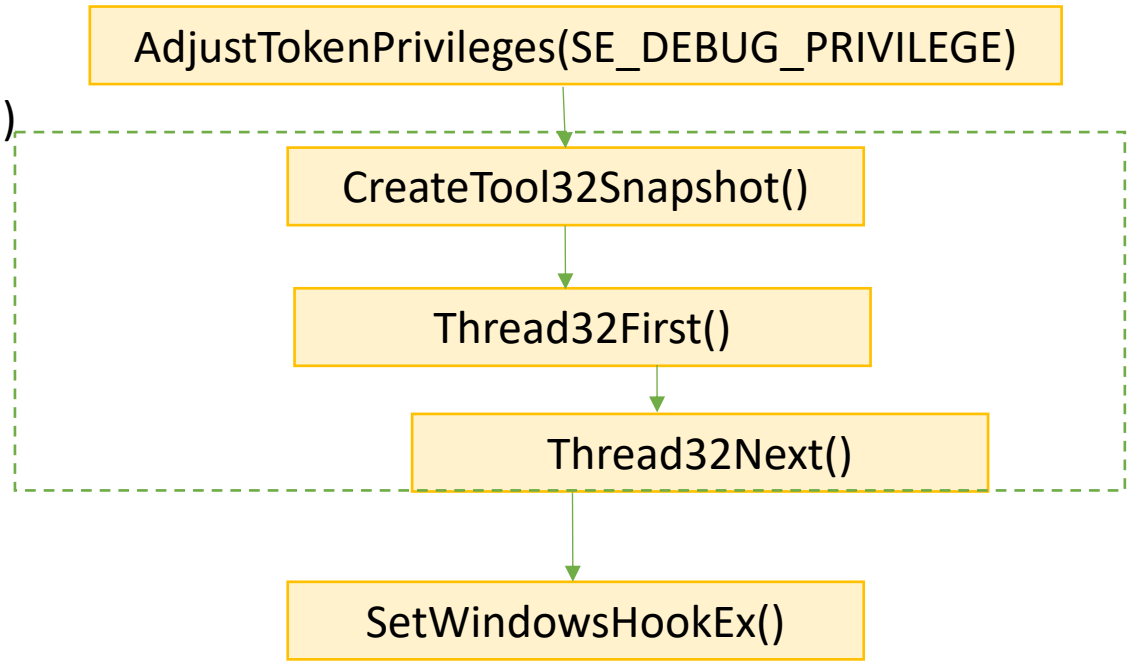
???

1. Классический
2. PE инъекция
3. Выкорчевывание
4. SIR (**S**uspend, **I**nject, **R**esume)
5. Hook



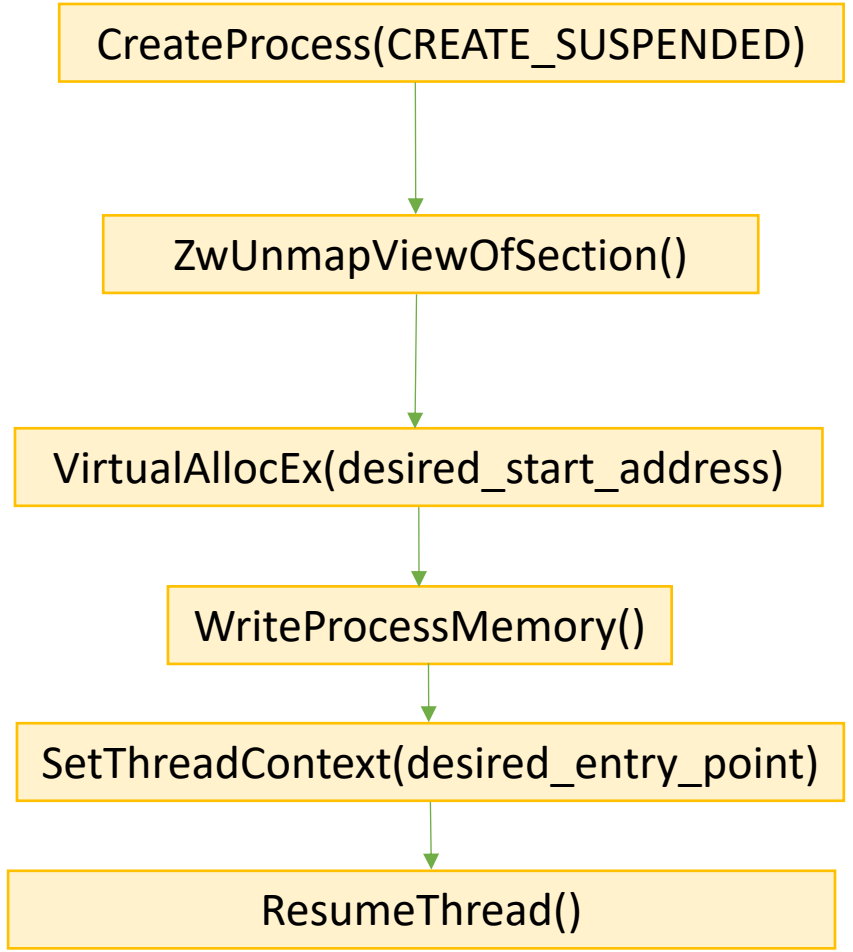
???

1. ~~Классический~~
2. PE инъекция
3. Выкорчевывание
4. SIR (**S**uspend, **I**nject, **R**esume)
5. Hook



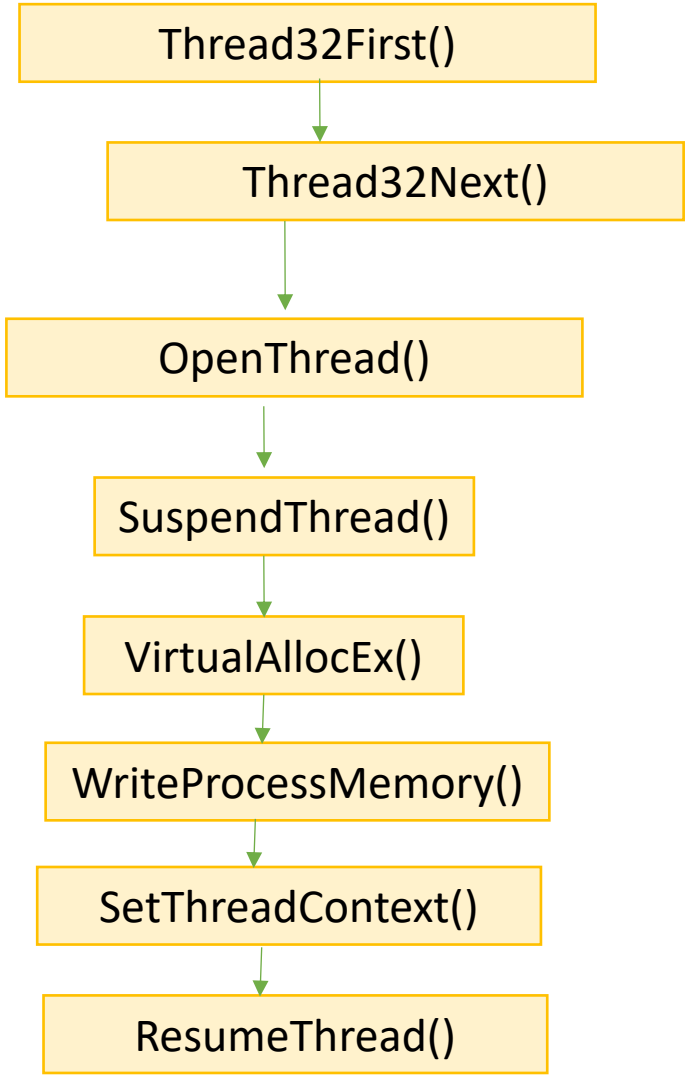
???

1. ~~Классический~~
2. PE инъекция
3. Выкорчевывание
4. SIR (**S**uspend, **I**nject, **R**esume)
5. ~~Hook~~



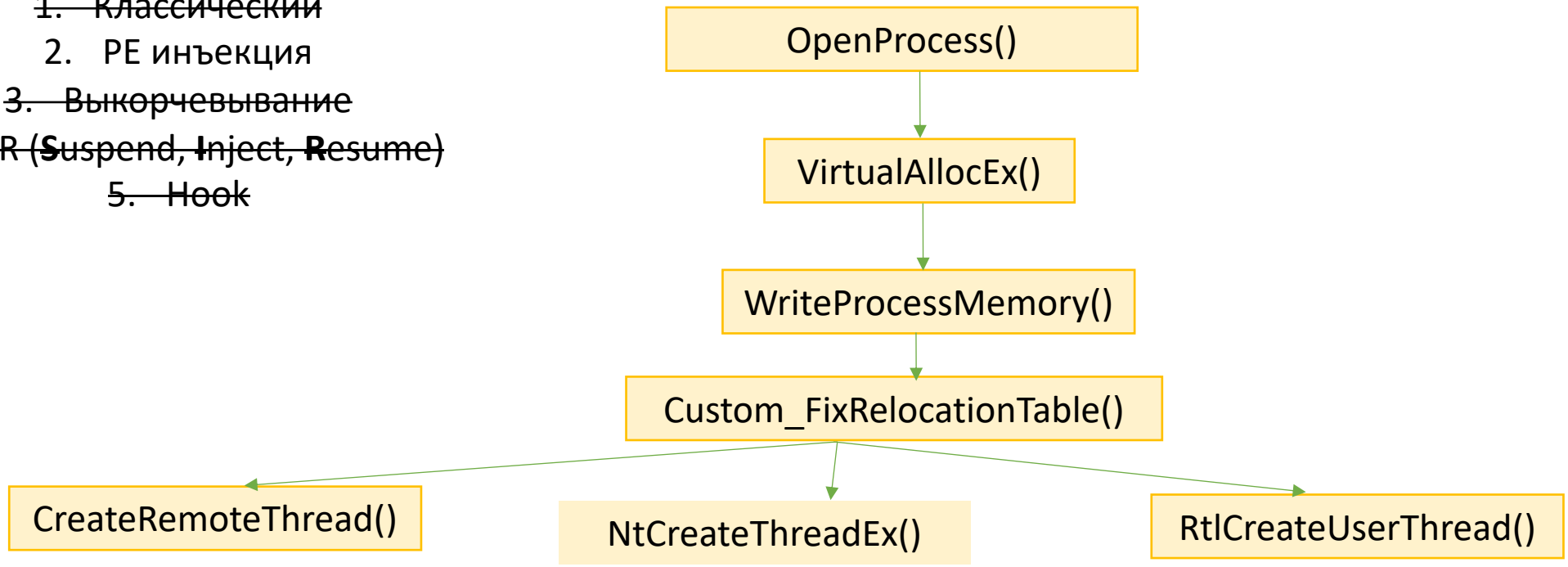
???

1. ~~Классический~~
2. PE инъекция
3. ~~Выкорчевывание~~
4. SIR (**S**uspend, **I**nject, **R**esume)
5. ~~Hook~~



???

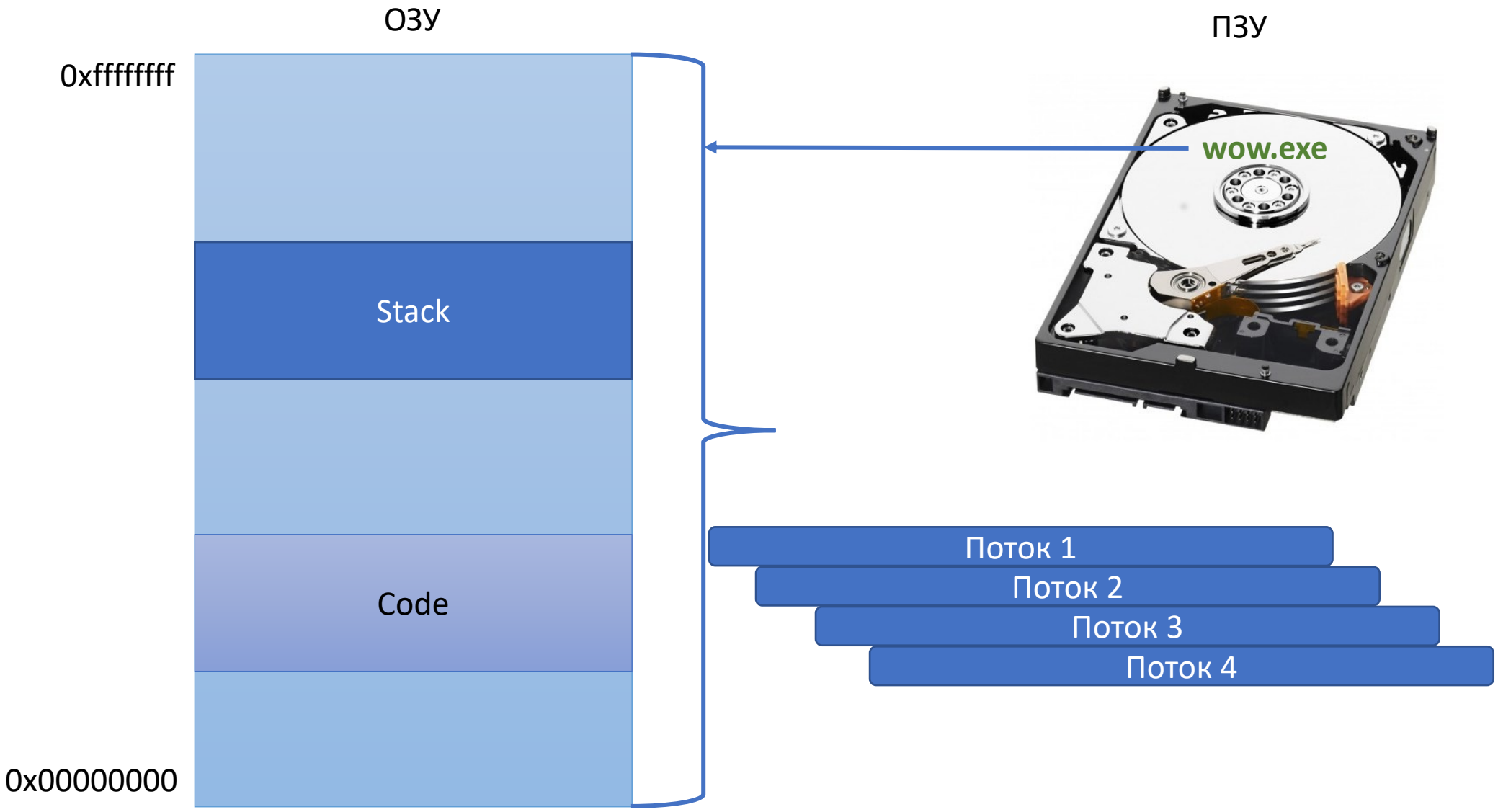
1. ~~Классический~~
2. PE инъекция
3. ~~Выкорчевывание~~
4. ~~SIR (**S**uspend, **I**nject, **R**esume)~~
5. ~~Hook~~



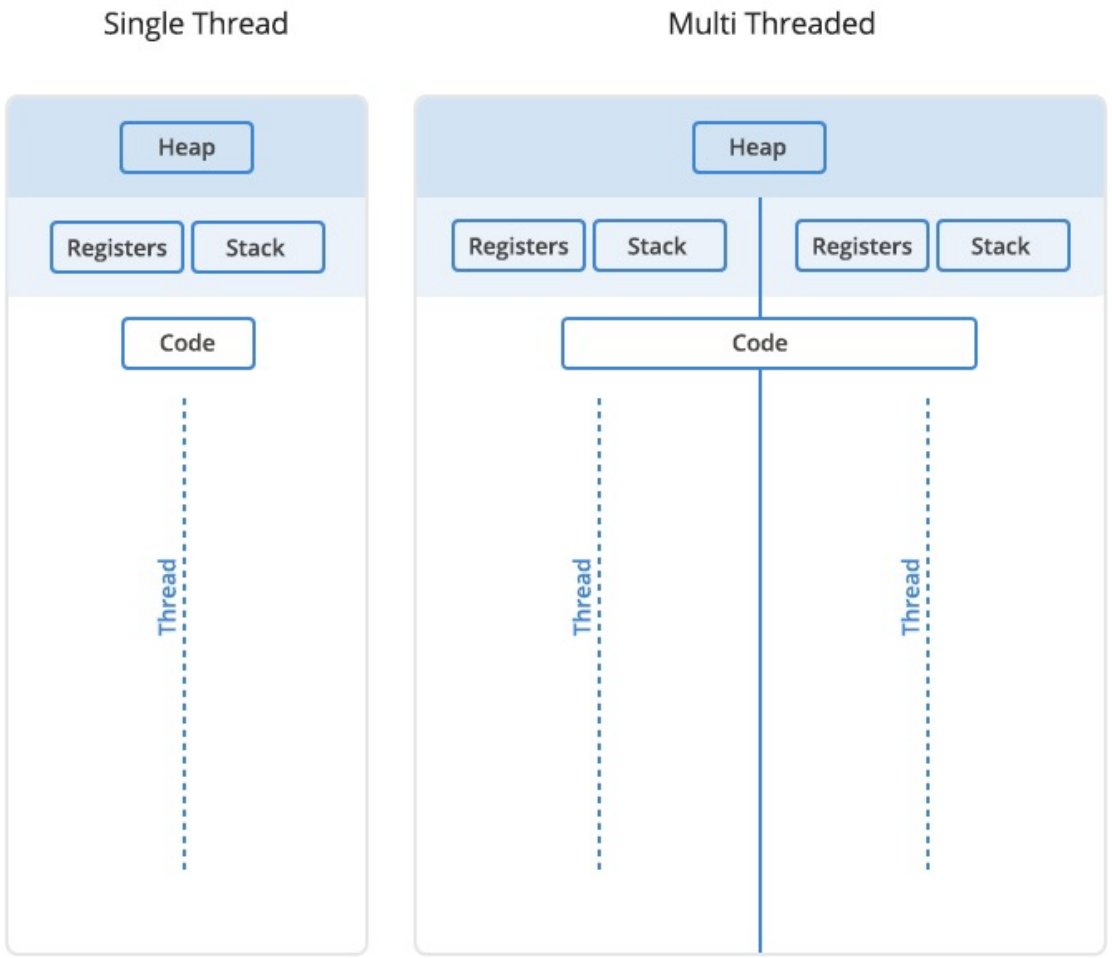
Какие еще есть способы?

- APC – Asynchronous Procedure Call
- EWMI
- SHIMS
- Userland rootkits

APC инъекция



APC инъекция

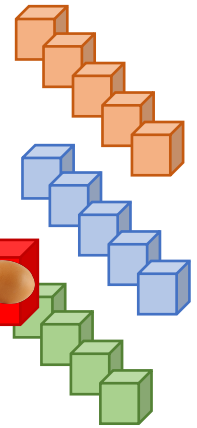


APC инъекция

APC очередь 1

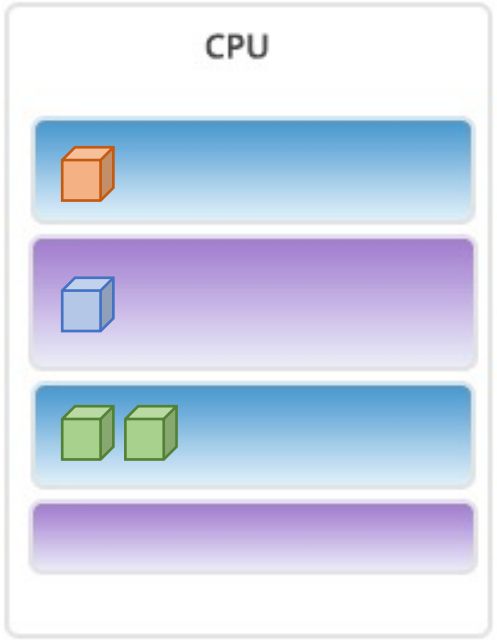
APC очередь 2

APC очередь 3

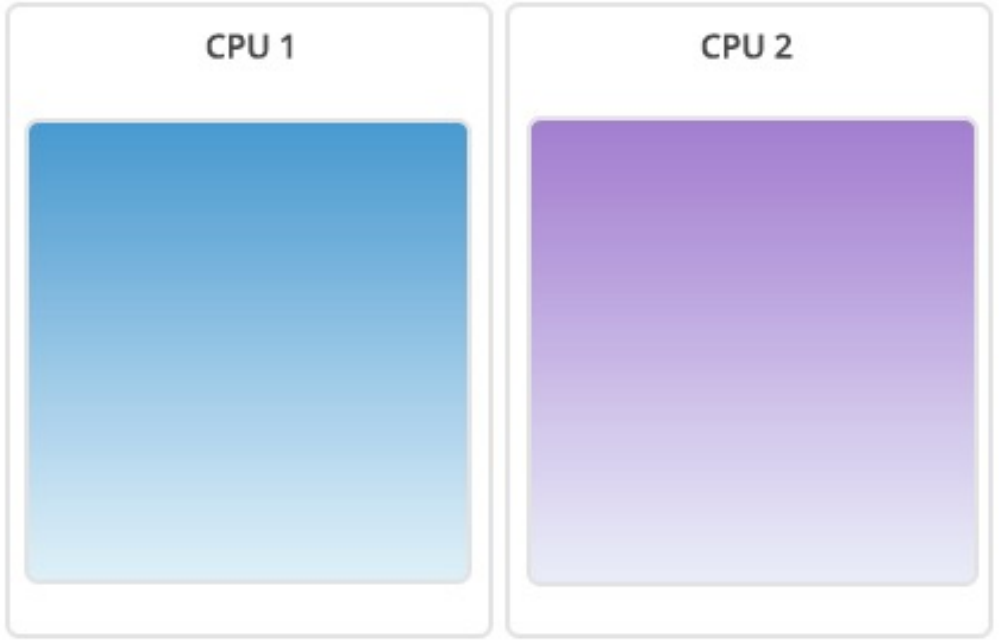


Injector

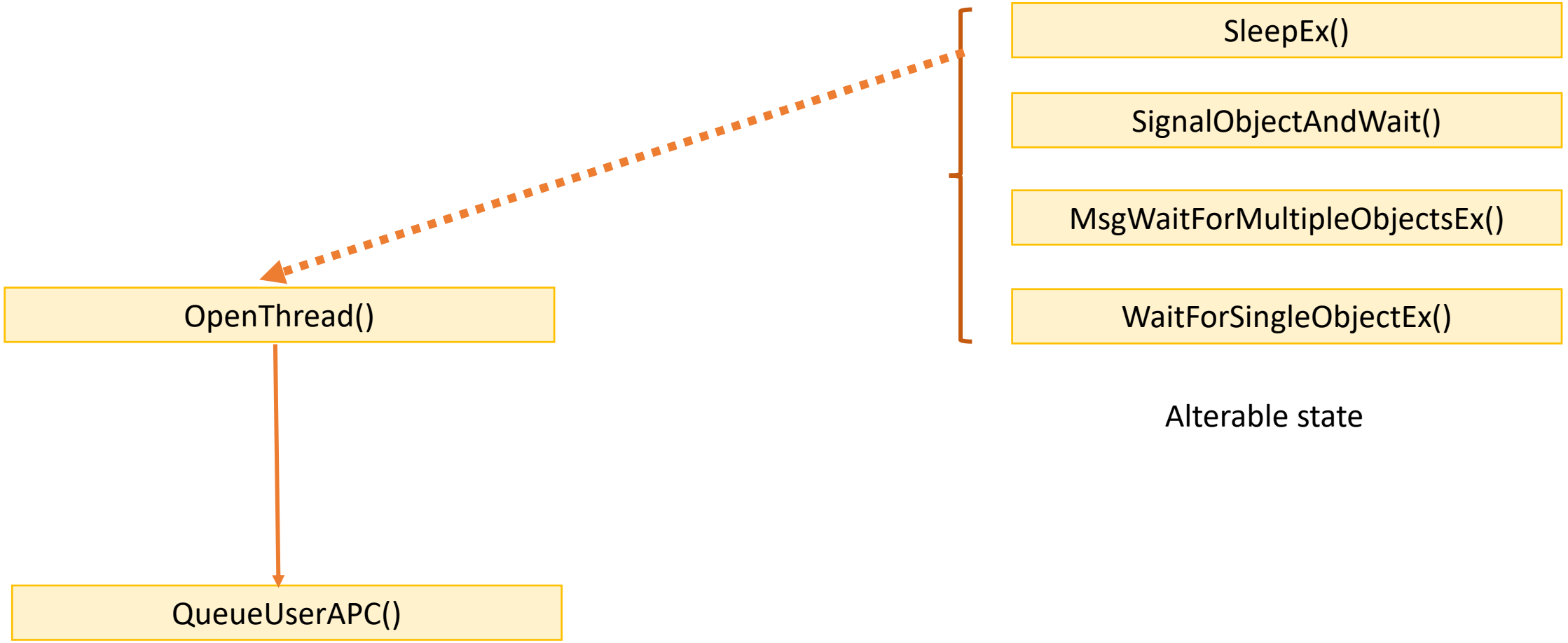
Concurrency



Parallelism



APC инъекция



APC инъекция

Параметр
для LoadLibrary()

OpenThread()

QueueUserAPC(thread_handle, fptr_LoadLibrary(), "C:/MyDocs/mal.dll")

Источники

Ten Process Injection Techniques: A Technical Survey Of Common And Trending Process Injection Techniques:

https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process