TDC2012
the developer's conference

Globalcode

Patch de Emergência

Wanderley Caloni

2012-07

C/C++

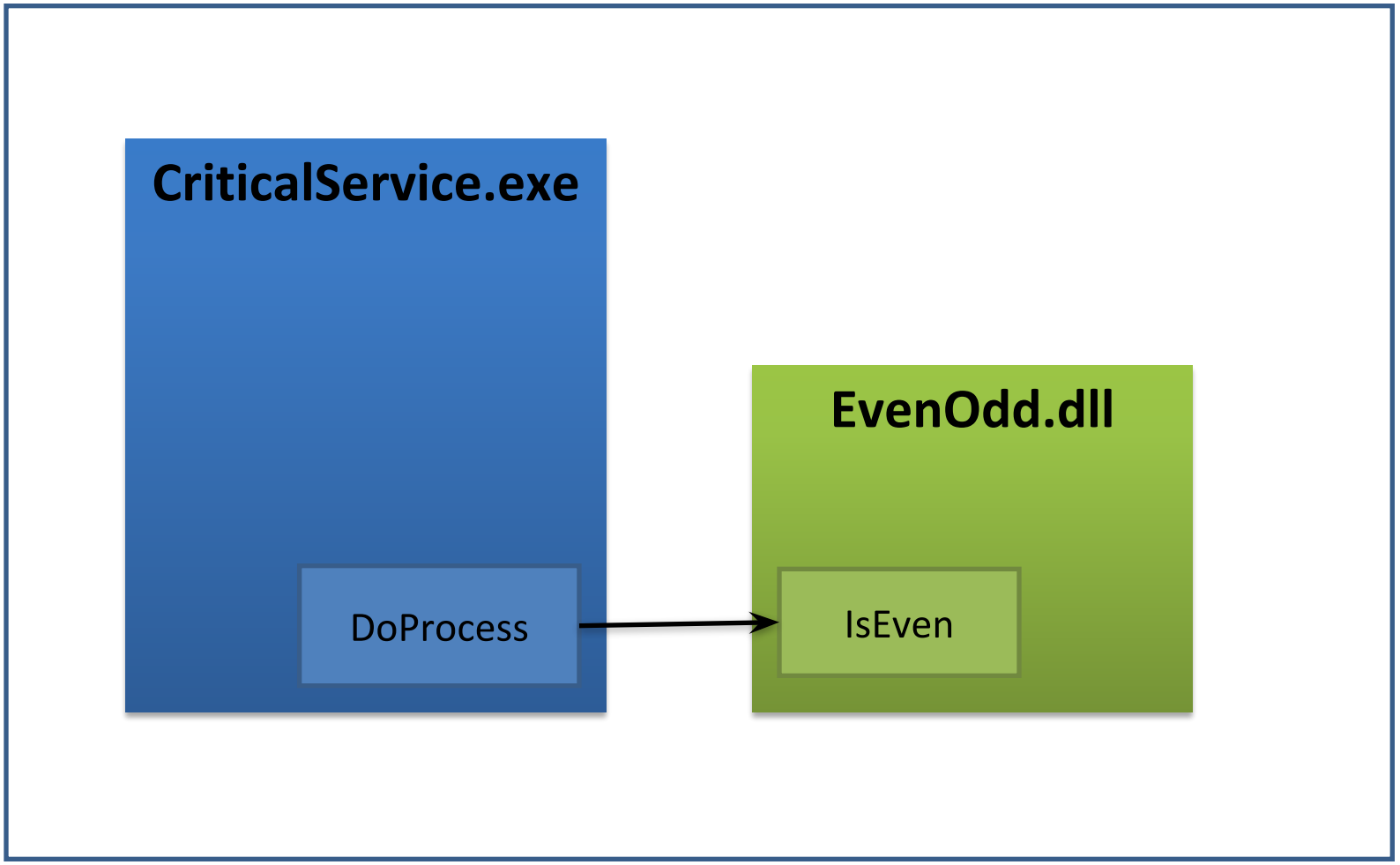
wanderley at caloni at low level

- Programador entusiasta (Basic YES!): 1 ano
- C/C++ Maniac: 2 anos
- Segurança da Informação: 10 anos
- Mercado Financeiro: 1 ano

wanderley at caloni at low level

Patch de Emergência

Espaço de memória do processo



Patch de Emergência

IsEven

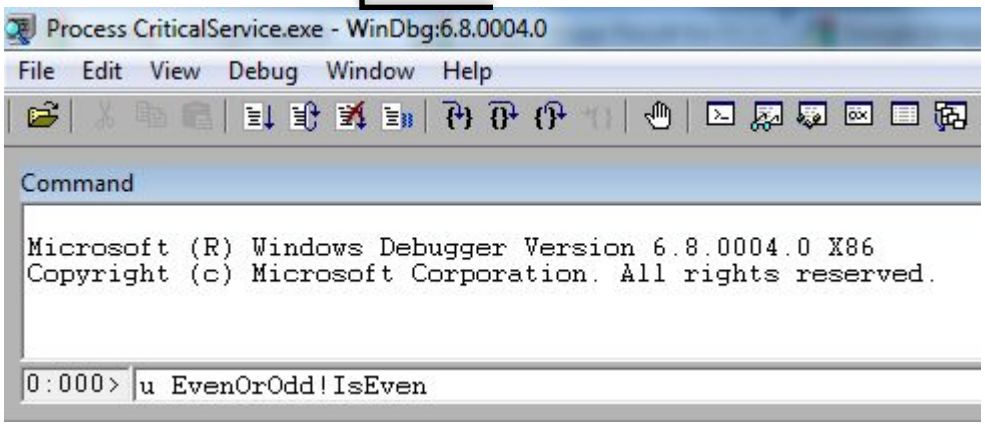
```
1001001001010
1010010101010
0010101011010
0101001101010
0010100101011
```

IsEven

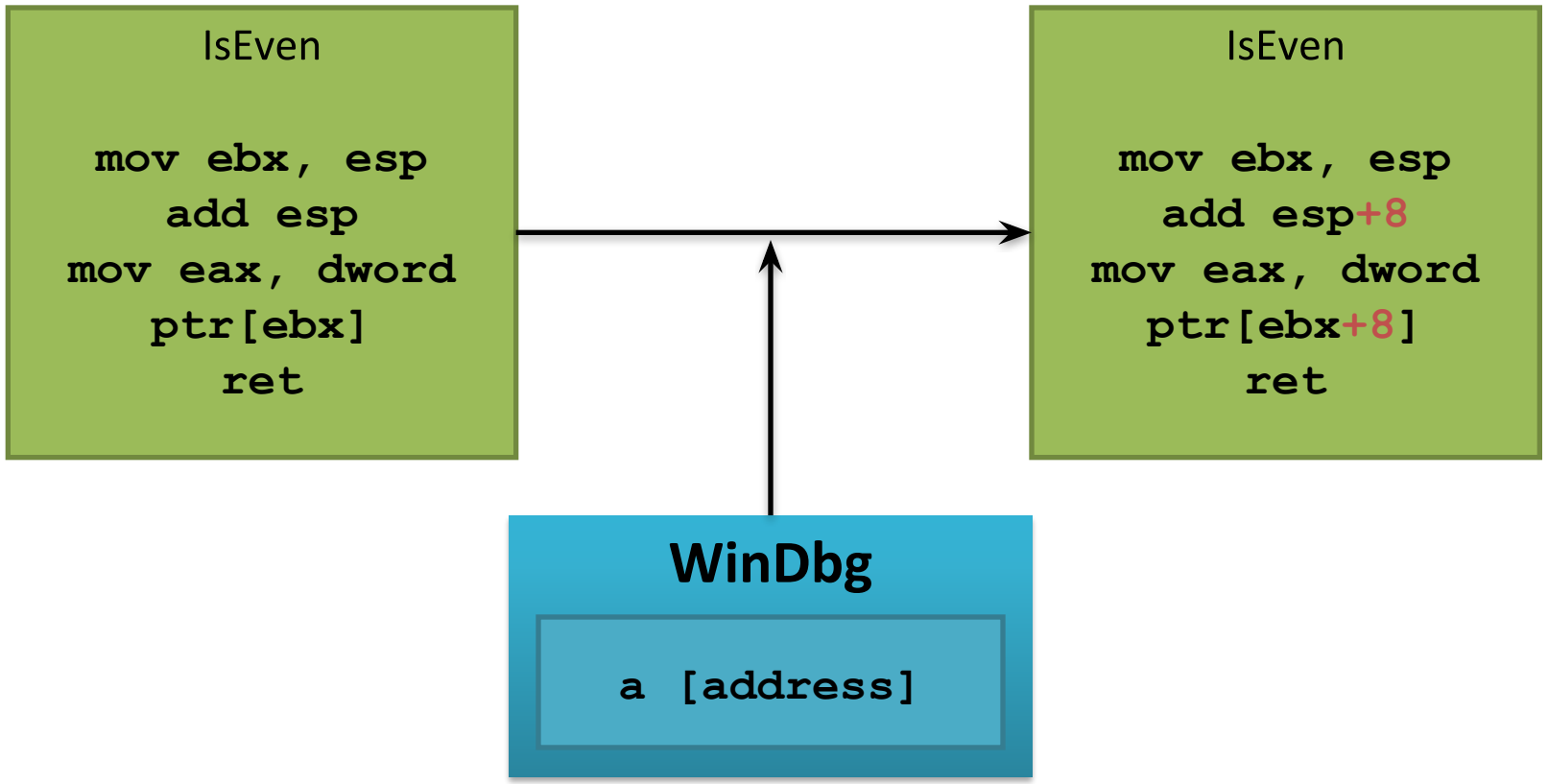
```
mov ebx, esp
add esp
mov eax, dword
ptr[ebx]
ret
```

windbg -pvr -pn CriticalService.exe

- nonin**V**asively
  Resume threads

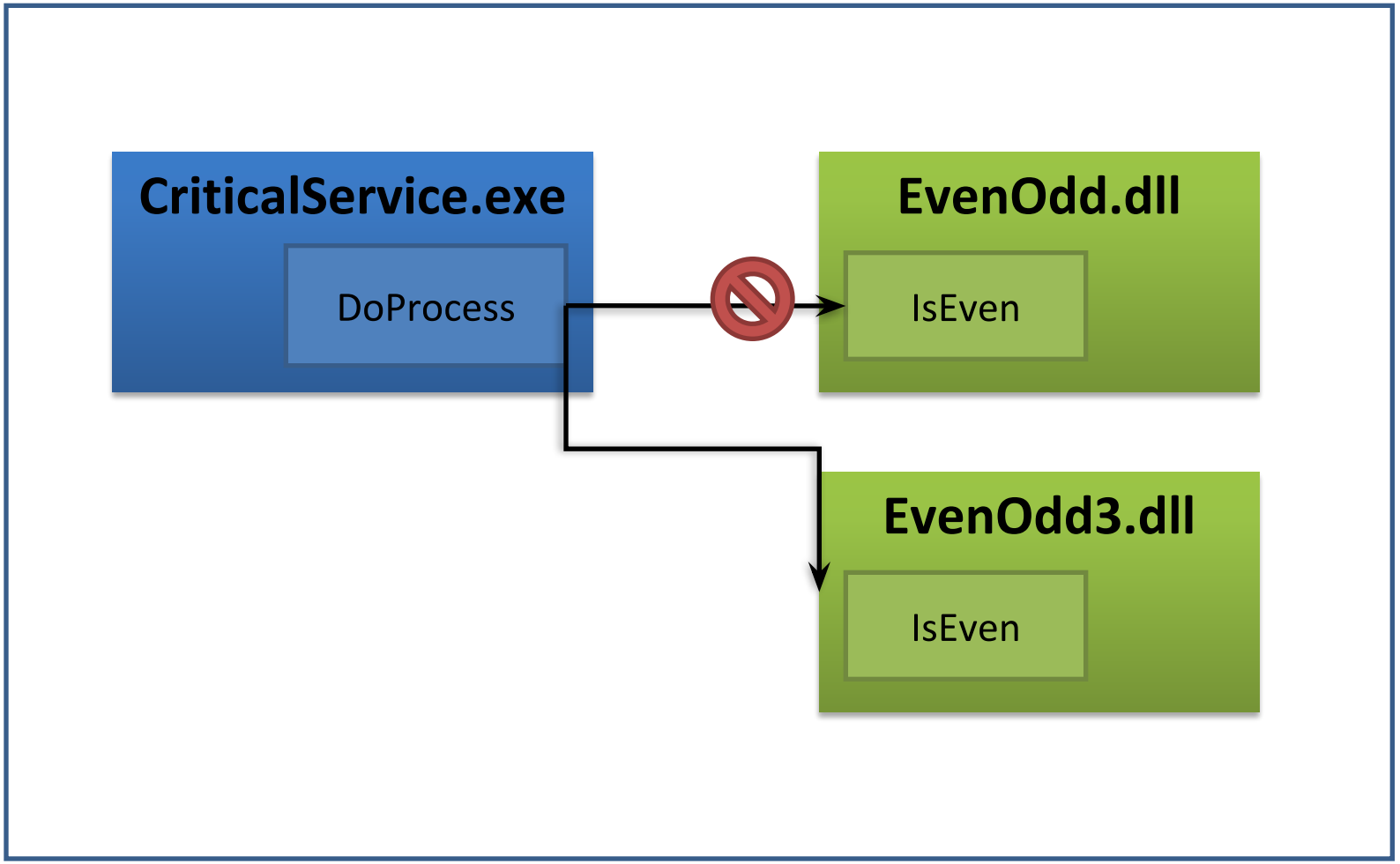


Patch de Emergência

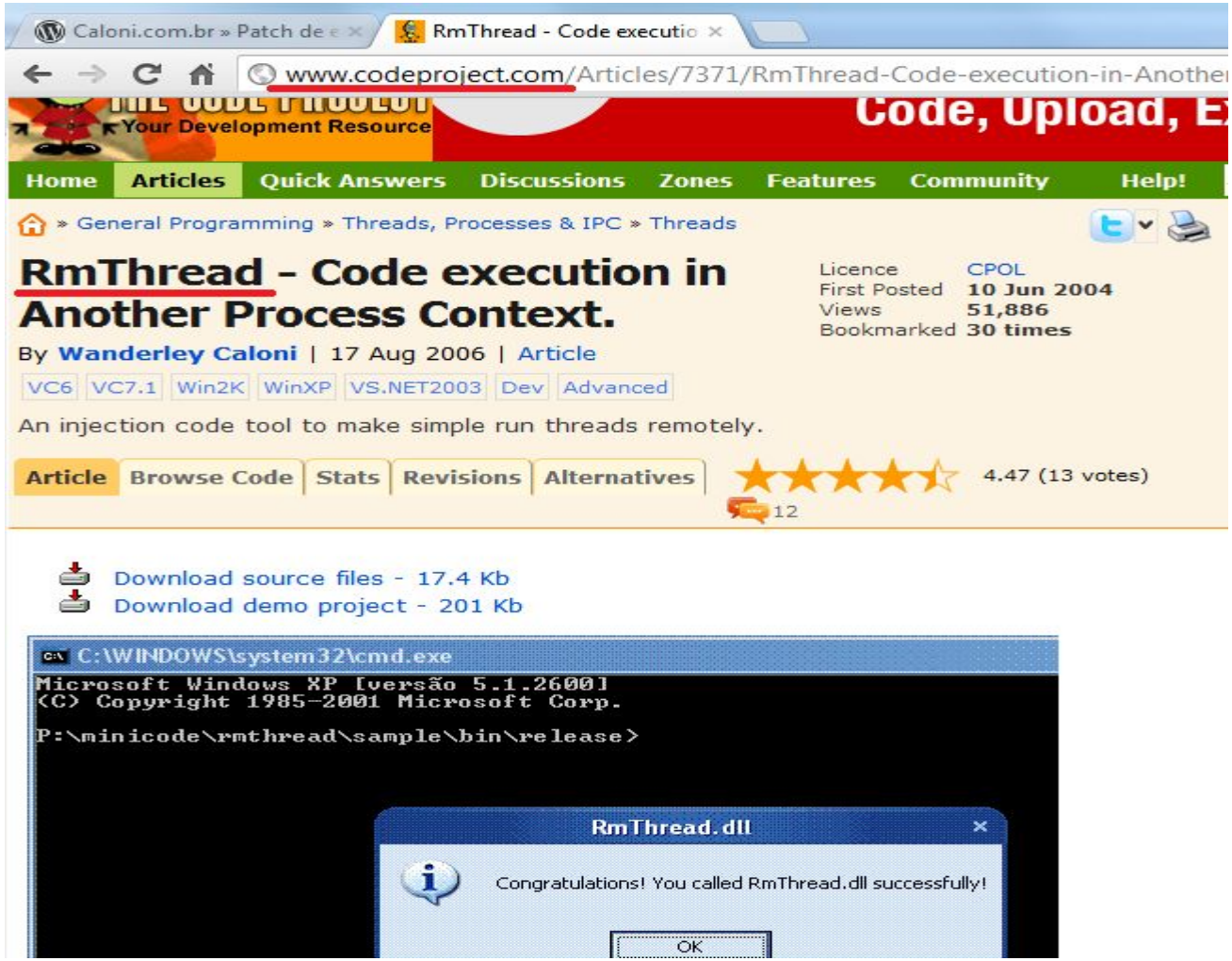


Patch de Emergência

Espaço de memória do processo

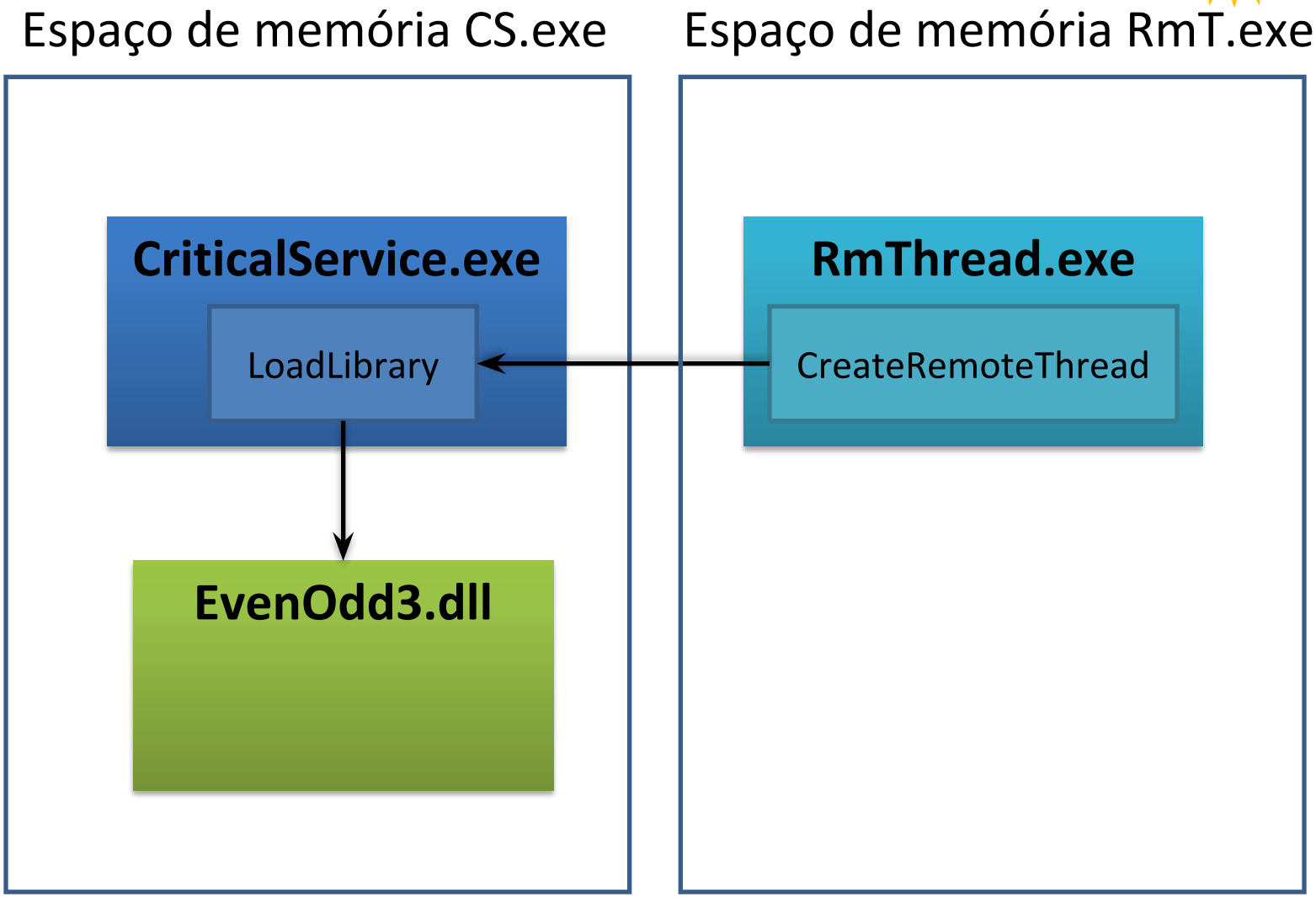


Patch de Emergência



Patch de Emergência

3.0!!



Patch de Emergência

Técnicas testadas

Técnicas documentadas

Técnicas automatizadas

KMJ: Keep My Job

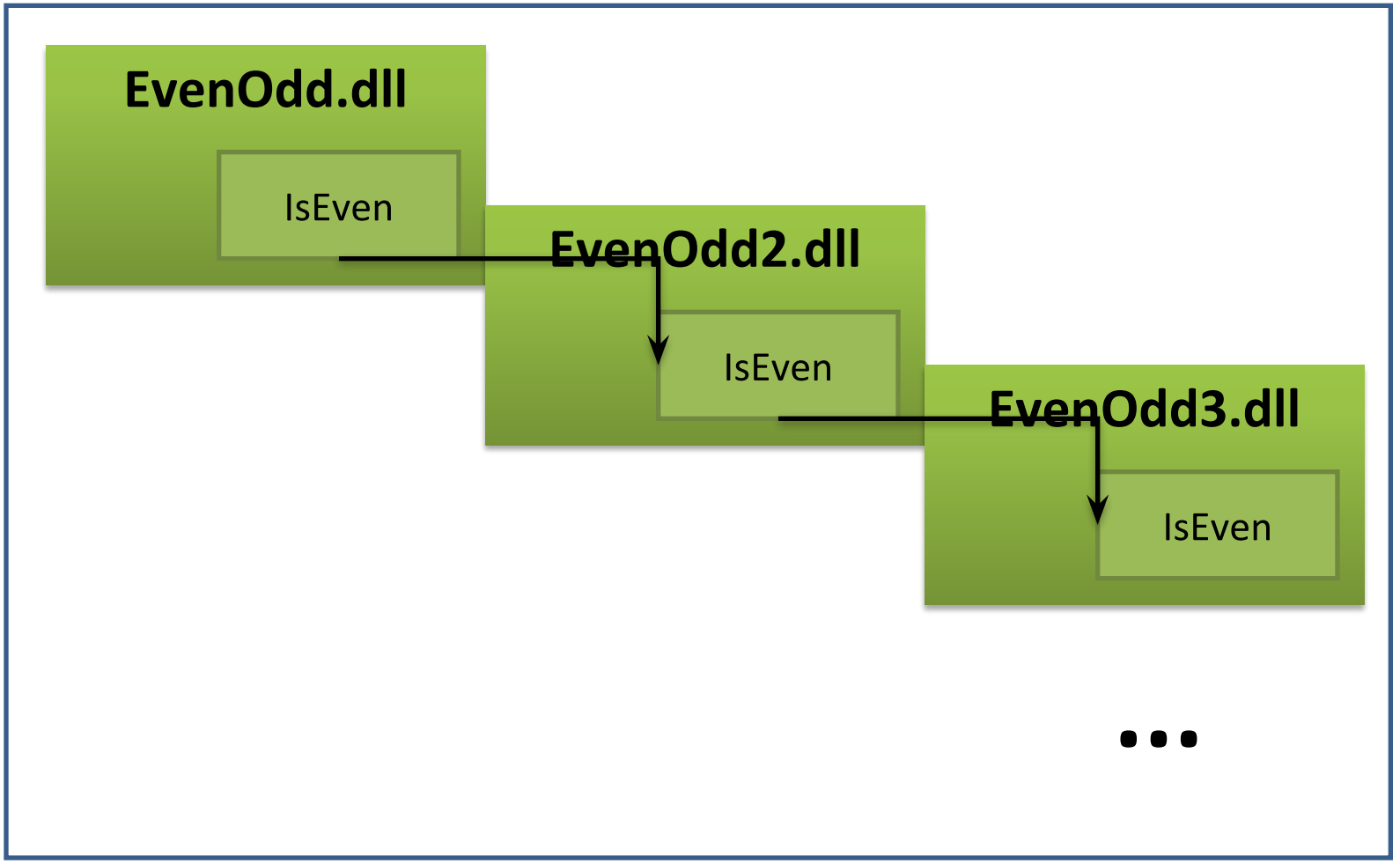
Jumps incondicionais

Carregamento dinâmico de DLLs

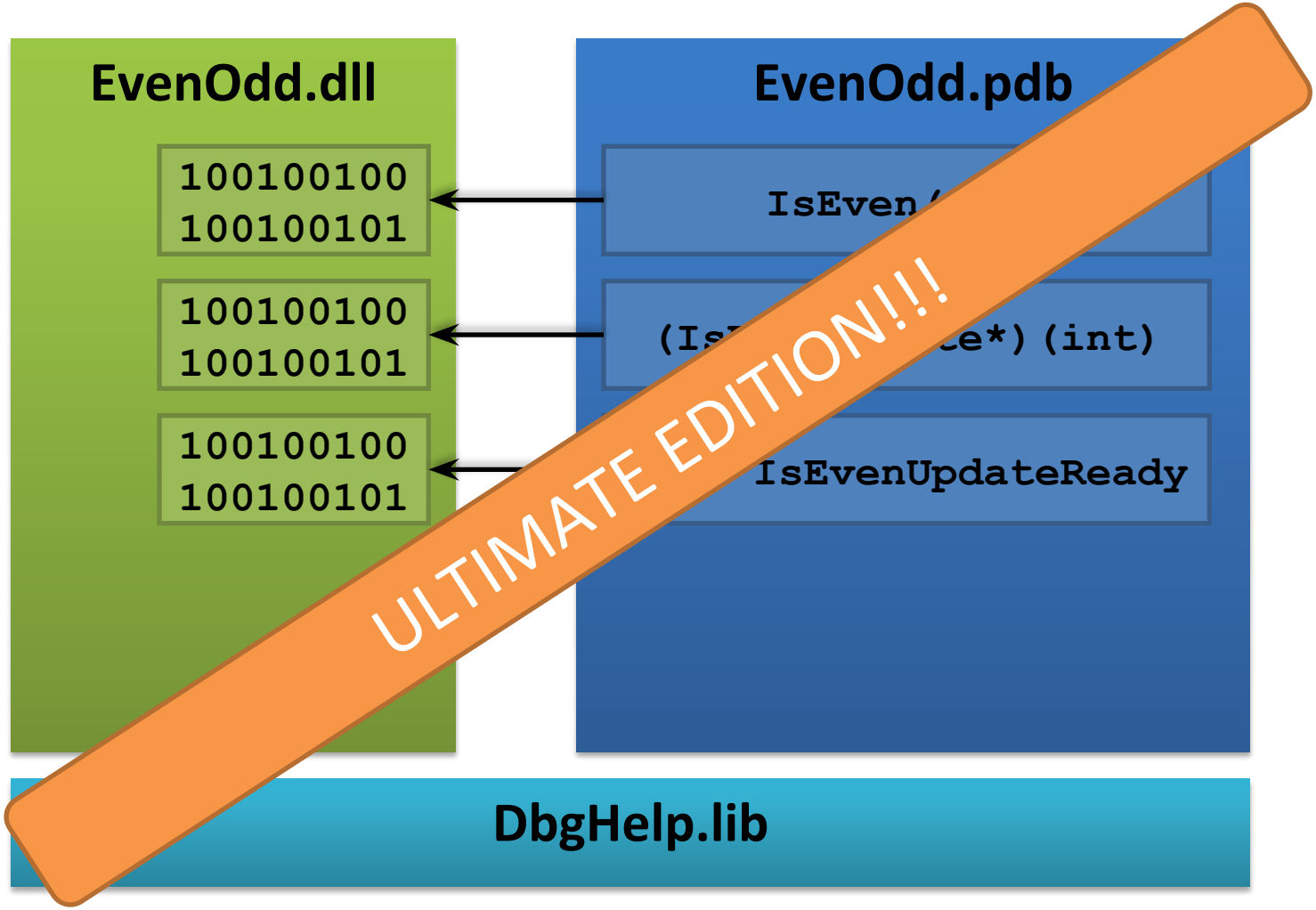
Escrita de assembly live

XGH: eXtreme
Go Horse Programming

Patch de Emergência



Patch de Emergência



O que aprendemos?

- ✔ ~~Aprender assembly e depuração é inútil~~
- ✔ Escrita de assembly inplace (tradução: na veia)
- ✔ Carregamento remoto de DLLs
- ✔ Solução alto nível para updates dinâmicos
- ✔ Update dinâmico feito auto-guiado

Dúvidas? Eu tenho várias.

e-mail

wanderley@caloni.com.br

twitter

saite