

Patch de Emergência

Wanderley Caloni

2012-07

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



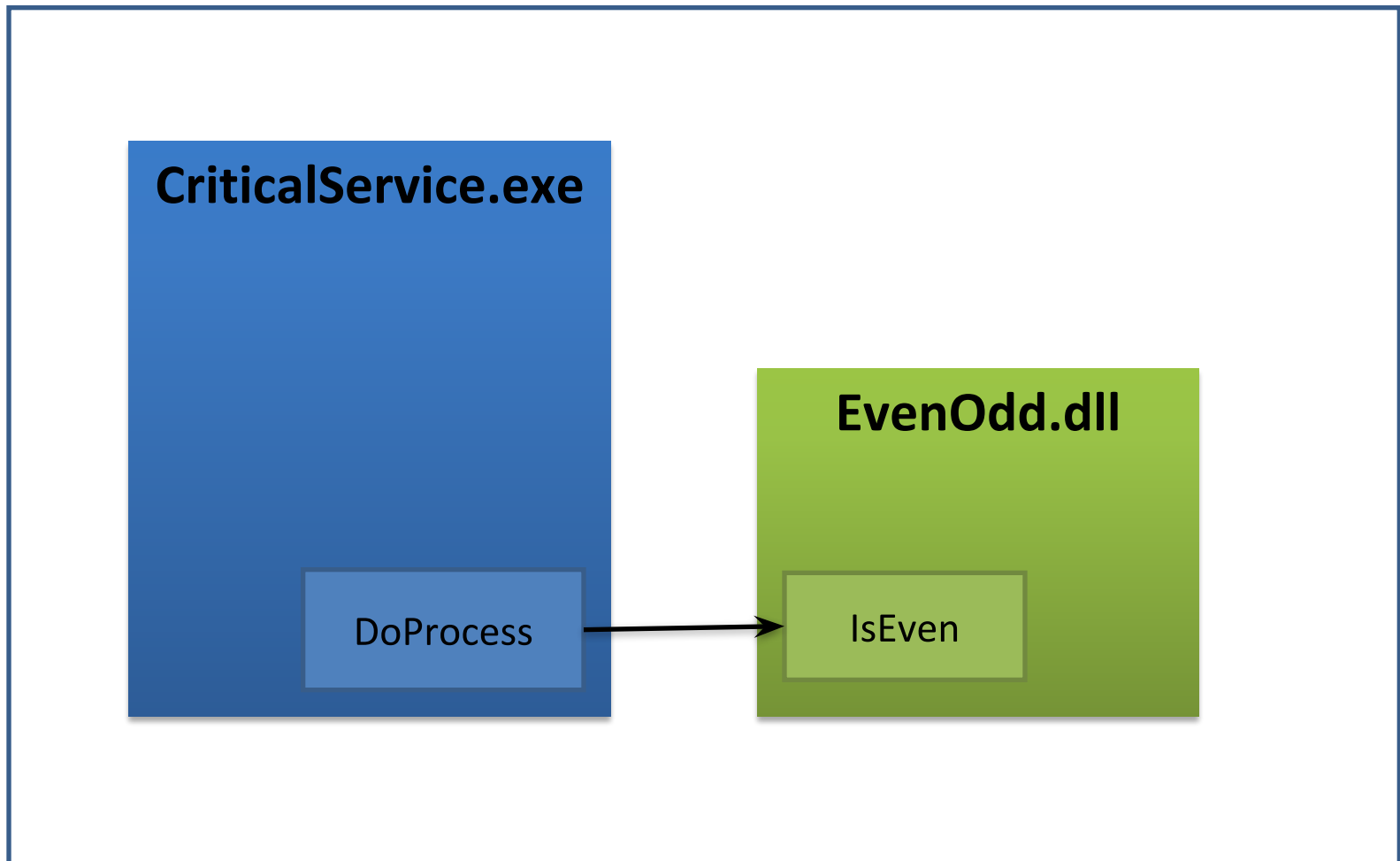
wanderley at caloni at low level





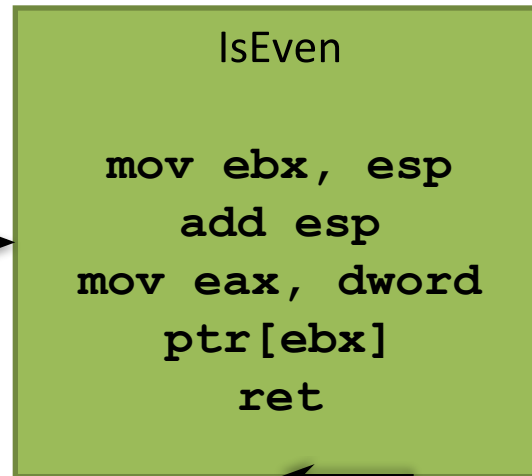
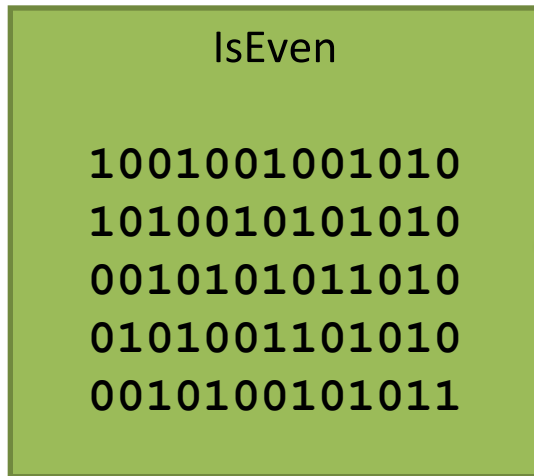
Patch de Emergência

Espaço de memória do processo



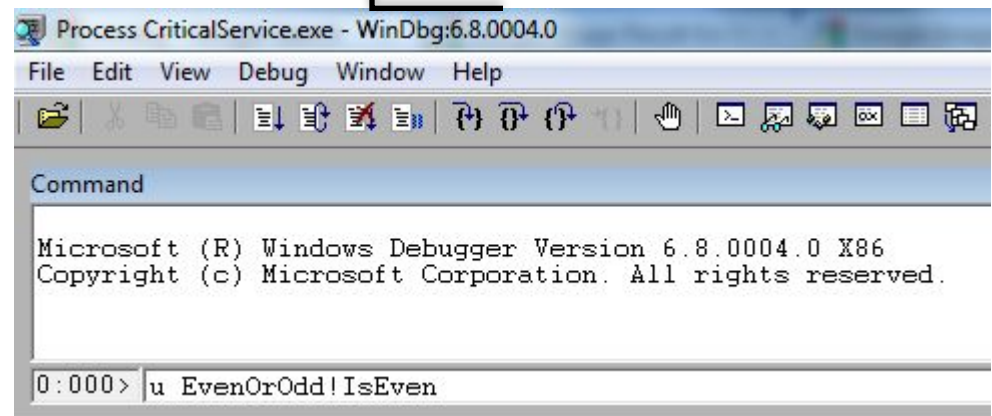


Patch de Emergência



windbg -pvr -pn CriticalService.exe

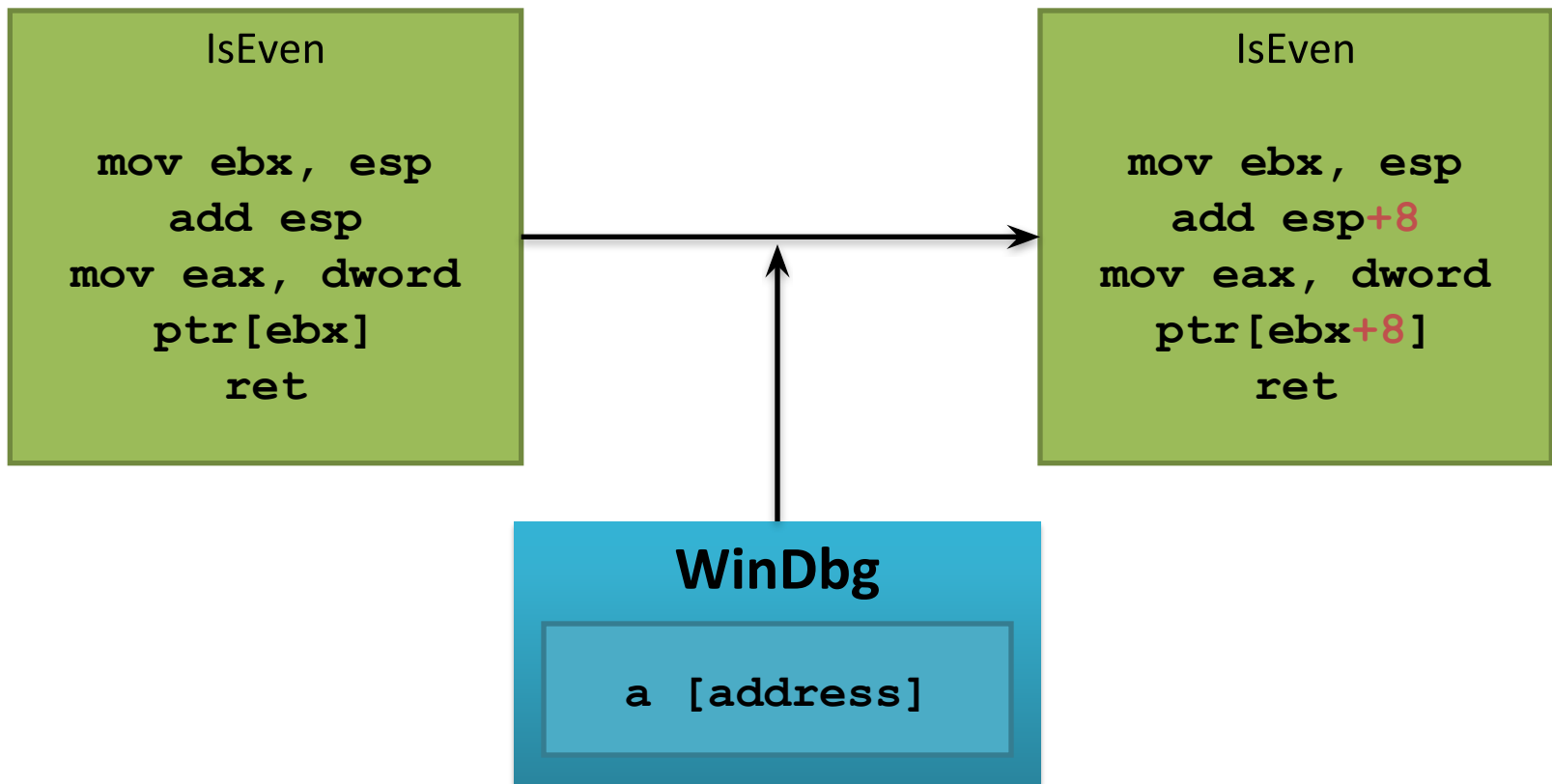
noninVasively
Resume threads





Patch de Emergência

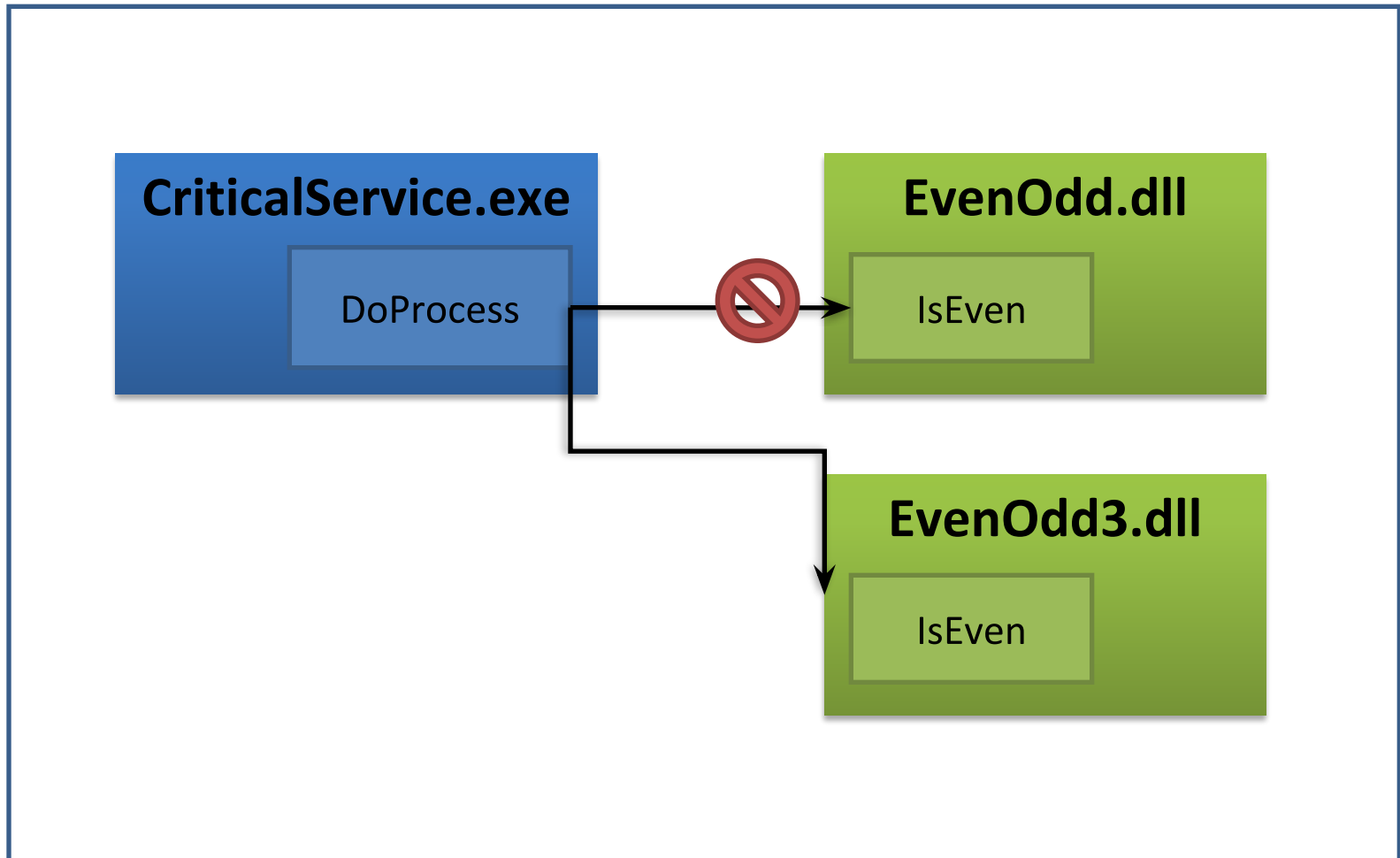
2.0!!





Patch de Emergência

Espaço de memória do processo





Patch de Emergência

Caloni.com.br » Patch de e x RmThread - Code executio x

← → ↻ ⌂ www.codeproject.com/Articles/7371/RmThread-Code-execution-in-Another

Code, Upload, E

Home Articles Quick Answers Discussions Zones Features Community Help!

» General Programming » Threads, Processes & IPC » Threads

RmThread - Code execution in Another Process Context.

By [Wanderley Caloni](#) | 17 Aug 2006 | [Article](#)

VC6 VC7.1 Win2K WinXP VS.NET2003 Dev Advanced

Licence CPOL
First Posted 10 Jun 2004
Views 51,886
Bookmarked 30 times

An injection code tool to make simple run threads remotely.

Article Browse Code Stats Revisions Alternatives

★★★★★ 4.47 (13 votes)

12

Download source files - 17.4 Kb
Download demo project - 201 Kb

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [versão 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
P:\minicode\rmthread\sample\bin\release>
```

RmThread.dll

i Congratulations! You called RmThread.dll successfully!

OK

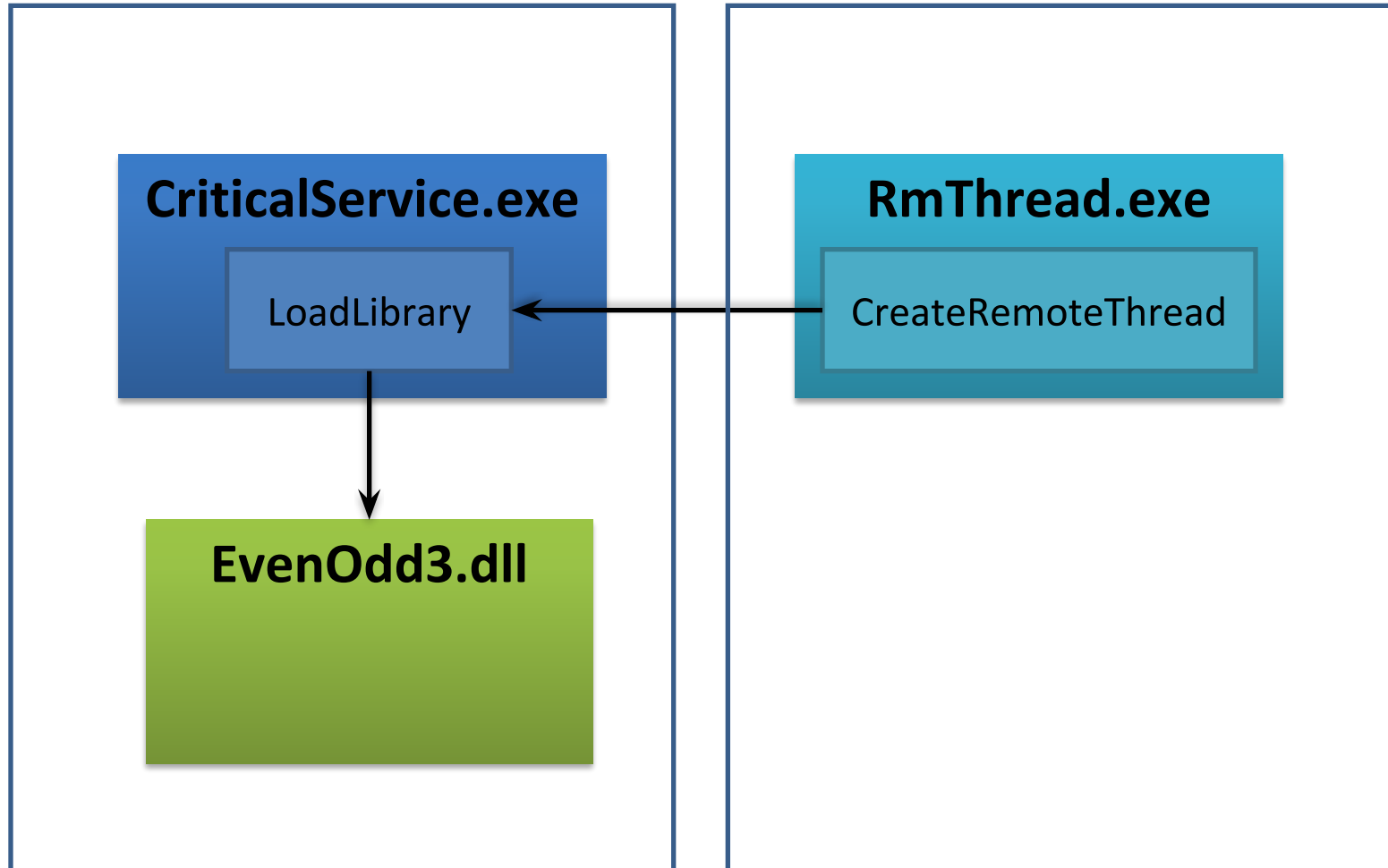


Patch de Emergência

3.0!!

Espaço de memória CS.exe

Espaço de memória RmT.exe





Patch de Emergência

Técnicas testadas

Técnicas documentadas

Técnicas automatizadas

KMJ: Keep My Job



Jumps incondicionais

Carregamento dinâmico de DLLs

Escrita de assembly live

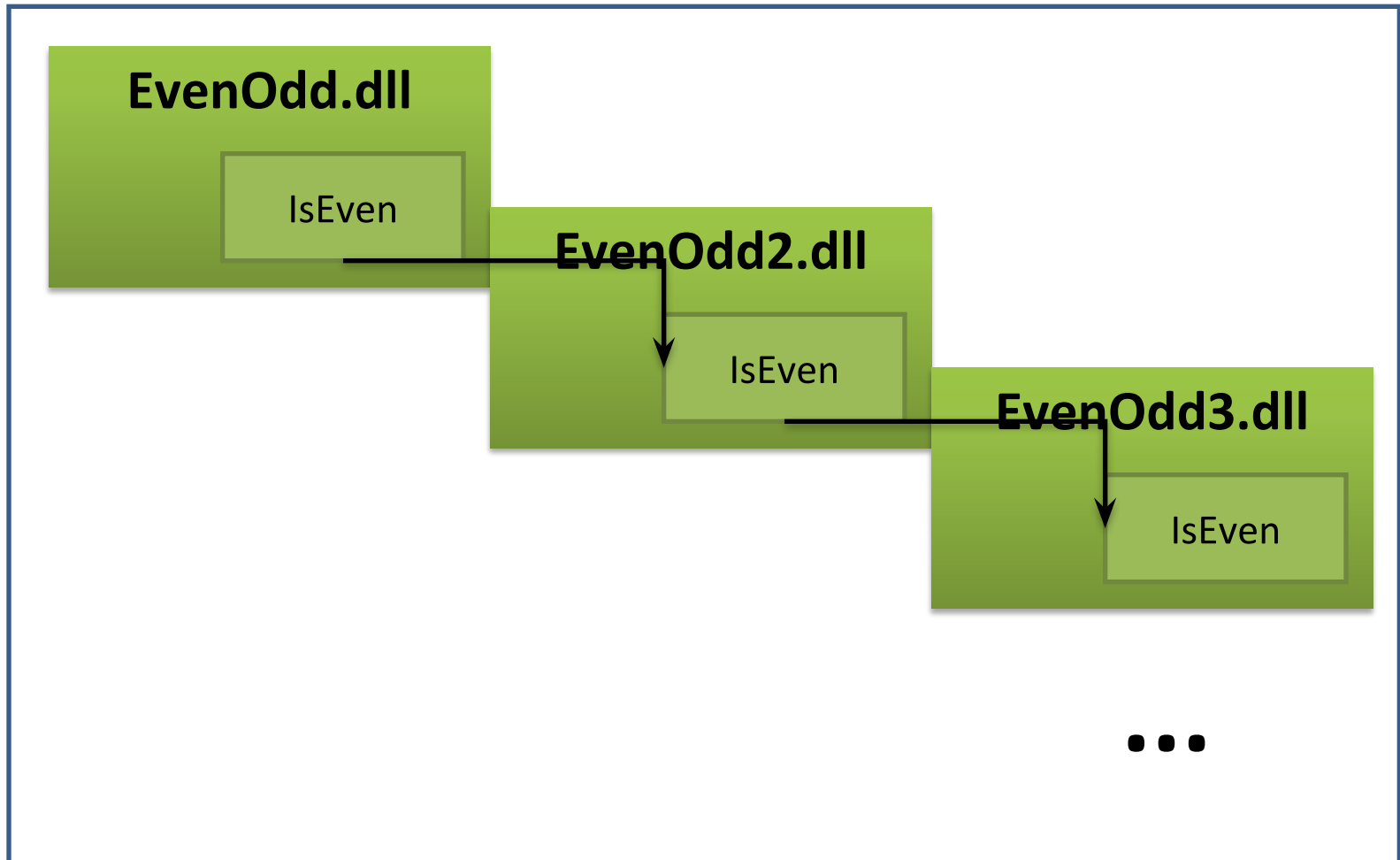
XGH: eXtreme
Go Horse Programming





Patch de Emergência

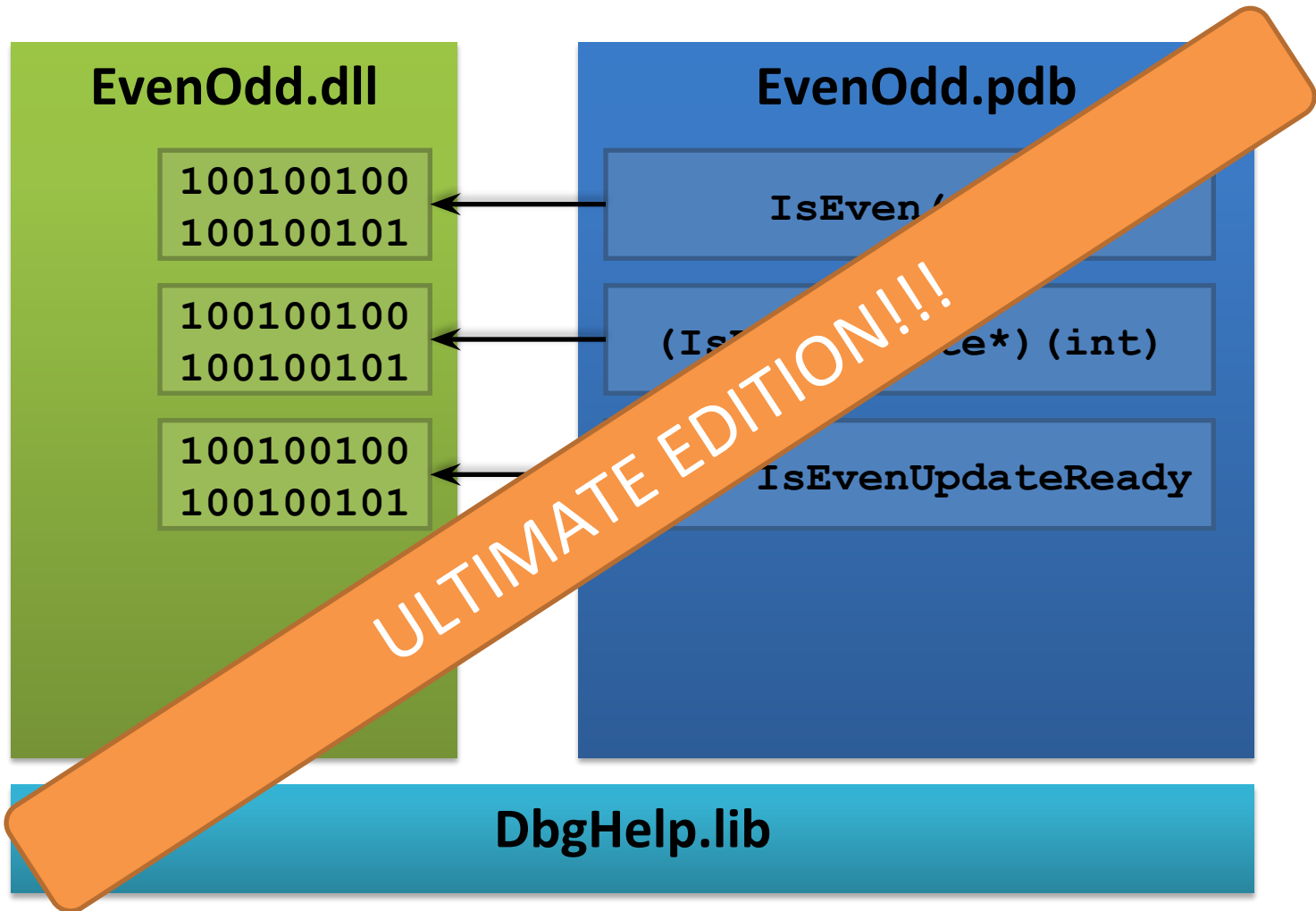
4.0!!





Patch de Emergência

5.0!!





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